Contents

Understanding SMB file access with Data ONTAP ................................. 15
   How namespaces and volume junctions affect SMB access on SVMs with
      FlexVol volumes .................................................................................................. 15
   What namespaces in SVMs with FlexVol volumes are ....................... 15
   Volume junction usage rules ......................................................................... 15
   How volume junctions are used in SMB and NFS namespaces .......... 16
   What the typical NAS namespace architectures are ............................ 16
LIF configuration requirements for file access management ...................... 19
   How security styles affect data access .............................................................. 20
   What the security styles and their effects are ............................................. 20
   Where and when to set security styles ......................................................... 21
   How to decide on what security style to use on SVMs with FlexVol
      volumes ........................................................................................................ 21
   How security style inheritance works ......................................................... 21
   How authentication provides SMB access security ........................................ 22
      Kerberos authentication ............................................................................. 22
      NTLM authentication ................................................................................. 23
   How name mapping is used to secure SMB file access on SVMs with FlexVol
      volumes ........................................................................................................ 23
   How name mapping works ......................................................................... 23
   How Data ONTAP secures file and directory access ................................... 24
   Role that export policies play with SMB access ......................................... 24
   Very large CIFS configuration changes might take some time to finish ...... 25

Configuring and managing Active Directory computer accounts for
SVMs (no CIFS license) ............................................................................... 26
   How to choose whether to create a CIFS server or an Active Directory computer
      account ......................................................................................................... 26
   Managing Active Directory computer accounts ....................................... 27
      Creating Active Directory computer accounts for SVMs ....................... 27
      Changing the Active Directory domain to which the SVM computer
         account is associated ........................................................................... 28
      Displaying information about Active Directory computer accounts for
         SVMs ...................................................................................................... 30
      Deleting Active Directory computer accounts for SVMs ....................... 30
      Changing or resetting Active Directory computer account passwords for
         SVMs ...................................................................................................... 31
   Managing domain controller connections for Active Directory computer
      accounts ....................................................................................................... 32
      Displaying information about discovered Active Directory servers for
         SVMs ...................................................................................................... 32
      Resetting and rediscovering Active Directory servers ............................ 33
Adding or removing preferred domain controllers ........................................... 34
Displaying information about preferred domain controllers ....................... 35

**Setting up CIFS servers** ................................................................. 36

How to choose whether to create a CIFS server or an Active Directory computer account ................................................................. 36
Supported SMB clients and domain controllers ........................................... 37
Unsupported Windows features ................................................................. 37
Prerequisites for CIFS server setup ........................................................... 37
Planning the CIFS server configuration ....................................................... 38
Information to gather before configuring time services ............................... 38
Information to gather before creating the IPspace, broadcast domain, and subnet configuration ......................................................... 39
Information to gather before configuring the SVM ...................................... 42
Information to gather before creating data LIFs on the SVM ........................... 44
Information to gather before configuring name services ............................. 45
Information to gather before creating the CIFS server ................................... 49

Setting up the CIFS server ........................................................................ 50
Configuring time services (cluster administrators only) ................................ 52
Creating an IPspace for the SVM (cluster administrators only) ..................... 52
Determining which ports can be used for a new broadcast domain (cluster administrators only) ................................................................. 53
Removing ports from an existing broadcast domain prior to adding them to the new broadcast domain (cluster administrators only) .......... 55
Creating a broadcast domain for the IPspace (cluster administrators only) ................................................................. 56
Creating a subnet for the IPspace (cluster administrators only) ..................... 57
Creating an SVM with FlexVol volumes for the CIFS server (cluster administrators only) ................................................................. 59
Creating LIFs on the SVM (cluster administrators only) ............................... 61
Configuring DNS services for the SVM ..................................................... 63
Configuring dynamic DNS on the SVM ..................................................... 64
Creating a CIFS server ............................................................................... 65
Configuring NIS or LDAP name services on the SVM ............................... 67

Where to find information about SMB support on Infinite Volumes .......... 69

**Managing CIFS servers** ................................................................. 70
Using options to customize CIFS servers .................................................. 70
Available CIFS server options .................................................................... 70
Configuring CIFS server options ............................................................... 74
Configuring access restrictions for anonymous users ................................ 74
Managing how file security is presented to SMB clients for UNIX security-style data ................................................................. 75
How to control automatic DFS advertisements in clustered Data ONTAP with a CIFS server option ................................................................. 77
Managing whether the CIFS server automatically advertises DFS capabilities ................................................................. 78
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing CIFS server security settings</td>
<td>79</td>
</tr>
<tr>
<td>Important considerations about CIFS server security settings in an SVM</td>
<td>79</td>
</tr>
<tr>
<td>disaster recovery configuration</td>
<td>79</td>
</tr>
<tr>
<td>Displaying information about CIFS server security settings</td>
<td>79</td>
</tr>
<tr>
<td>Enabling or disabling required password complexity for local SMB</td>
<td>79</td>
</tr>
<tr>
<td>users</td>
<td>80</td>
</tr>
<tr>
<td>Modifying the CIFS server Kerberos security settings</td>
<td>81</td>
</tr>
<tr>
<td>Setting the CIFS server minimum authentication security level</td>
<td>83</td>
</tr>
<tr>
<td>Configuring strong security for Kerberos-based communication by using</td>
<td>83</td>
</tr>
<tr>
<td>AES encryption</td>
<td>83</td>
</tr>
<tr>
<td>Using SMB signing to enhance network security</td>
<td>85</td>
</tr>
<tr>
<td>Configuring required SMB encryption on CIFS servers for data transfers</td>
<td>92</td>
</tr>
<tr>
<td>over SMB</td>
<td>95</td>
</tr>
<tr>
<td>Using LDAP over SSL/TLS to secure communication</td>
<td>99</td>
</tr>
<tr>
<td>Configuring default Windows user to UNIX user mappings on the CIFS server</td>
<td>99</td>
</tr>
<tr>
<td>Configuring the default UNIX user</td>
<td>99</td>
</tr>
<tr>
<td>Configuring the guest UNIX user</td>
<td>100</td>
</tr>
<tr>
<td>Mapping the administrators group to root</td>
<td>101</td>
</tr>
<tr>
<td>Displaying information about what types of users are connected over SMB</td>
<td>102</td>
</tr>
<tr>
<td>sessions</td>
<td>103</td>
</tr>
<tr>
<td>Configuring SMB on your CIFS server</td>
<td>103</td>
</tr>
<tr>
<td>Supported SMB versions</td>
<td>103</td>
</tr>
<tr>
<td>Enabling or disabling SMB 2.x</td>
<td>106</td>
</tr>
<tr>
<td>Enabling or disabling SMB 3.0</td>
<td>107</td>
</tr>
<tr>
<td>Improving client performance with traditional and lease oplocks</td>
<td>107</td>
</tr>
<tr>
<td>Write cache data-loss considerations when using oplocks</td>
<td>108</td>
</tr>
<tr>
<td>Enabling or disabling oplocks when creating SMB shares</td>
<td>108</td>
</tr>
<tr>
<td>Enabling or disabling oplocks on existing SMB shares</td>
<td>109</td>
</tr>
<tr>
<td>Commands for enabling or disabling oplocks on volumes and qtrees</td>
<td>110</td>
</tr>
<tr>
<td>Monitoring oplock status</td>
<td>111</td>
</tr>
<tr>
<td>Applying Group Policy Objects to CIFS servers</td>
<td>113</td>
</tr>
<tr>
<td>Supported GPOs</td>
<td>113</td>
</tr>
<tr>
<td>Requirements for using GPOs with your CIFS server</td>
<td>118</td>
</tr>
<tr>
<td>Enabling or disabling GPO support on a CIFS server</td>
<td>118</td>
</tr>
<tr>
<td>How GPOs are updated on the CIFS server</td>
<td>119</td>
</tr>
<tr>
<td>Manually updating GPO settings on the CIFS server</td>
<td>120</td>
</tr>
<tr>
<td>Displaying information about GPO configurations</td>
<td>120</td>
</tr>
<tr>
<td>Displaying detailed information about restricted group GPOs</td>
<td>123</td>
</tr>
<tr>
<td>Displaying information about central access policies</td>
<td>125</td>
</tr>
<tr>
<td>Displaying information about central access policy rules</td>
<td>126</td>
</tr>
<tr>
<td>Changing CIFS servers computer account passwords</td>
<td>128</td>
</tr>
<tr>
<td>Changing or resetting the domain account password</td>
<td>128</td>
</tr>
<tr>
<td>Configuring CIFS servers for automatic computer account password</td>
<td>128</td>
</tr>
<tr>
<td>changes</td>
<td>128</td>
</tr>
</tbody>
</table>
Disabling automatic computer account password changes on CIFS servers .............................................................. 129
Managing domain controller connections ................................................................. 130
Displaying information about discovered servers .............................................. 130
Resetting and rediscovering servers ................................................................. 130
Adding preferred domain controllers ................................................................. 131
Commands for managing preferred domain controllers ................................. 132
Managing NetBIOS aliases for CIFS servers .......................................................... 132
Adding a list of NetBIOS aliases to the CIFS server ........................................ 132
Removing NetBIOS aliases from the NetBIOS alias list ............................... 133
Displaying the list of NetBIOS aliases on CIFS servers ........................................ 134
Determining whether SMB clients are connected using NetBIOS aliases .................................................. 135
Managing miscellaneous CIFS server tasks ............................................................ 135
Modifying protocols for SVMs ................................................................... 136
Stopping or starting the CIFS server ................................................................. 136
Moving CIFS servers to different OUs ............................................................... 137
Modifying the dynamic DNS domain on the SVM before moving the CIFS server .......................................................................................................................... 138
Joining an SVM to an Active Directory domain ............................................. 139
Displaying information about NetBIOS over TCP connections .................... 140
Commands for managing CIFS servers .............................................................. 140
Using IPv6 for SMB access and CIFS services .................................................... 141
Requirements for using IPv6 ....................................................................... 141
Support for IPv6 with SMB access and CIFS services ........................................ 142
How CIFS servers use IPv6 to connect to external servers ................................ 143
Enabling IPv6 for SMB (cluster administrators only) ........................................ 144
How to disable IPv6 for SMB ..................................................................... 144
Monitoring and displaying information about IPv6 SMB sessions .................... 144
Setting up file access using SMB ........................................................................ 145
File and directory naming dependencies in a multiprotocol environment ............... 145
Characters a file or directory name can use ...................................................... 145
How clustered Data ONTAP creates file and directory names ....................... 145
Case-sensitivity of file and directory names in a multiprotocol environment .............................................................................................. 145
Configuring security styles ...................................................................................... 146
Configuring security styles on SVM root volumes ........................................... 147
Configuring security styles on FlexVol volumes .............................................. 147
Configuring security styles on qtrees ............................................................... 147
Creating and managing data volumes in NAS namespaces .............................. 148
Creating data volumes with specified junction points ..................................... 148
Creating data volumes without specifying junction points ............................. 149
Mounting or unmounting existing volumes in the NAS namespace ............... 150
Displaying volume mount and junction point information ............................ 151
Securing file access by using Storage-Level Access Guard .............................. 152
Use cases for using Storage-Level Access Guard ............................................. 153
Workflow to configure Storage-Level Access Guard .................................. 153
Configuring Storage-Level Access Guard ................................................... 154
Displaying information about Storage-Level Access Guard ....................... 158
Removing Storage-Level Access Guard ..................................................... 160

Configuring character mapping for SMB file name translation on FlexVol
volumes .............................................................................................................. 161

Commands for managing character mappings for SMB file name
translation .............................................................................................................. 163

Creating name mappings ............................................................................. 163
Name mapping conversion rules .................................................................... 164
Creating a name mapping ............................................................................ 165
Commands for managing name mappings .................................................. 166

Configuring multidomain name-mapping searches ........................................ 166
Multidomain searches for UNIX user to Windows user name mappings .... 166
Enabling or disabling multidomain name mapping searches ...................... 166
Resetting and rediscovering trusted domains .............................................. 168
Displaying information about discovered trusted domains ......................... 170
Adding, removing, or replacing trusted domains in preferred trusted
domain lists ................................................................................................. 170
Displaying information about the preferred trusted domain list ................. 171

Creating and configuring SMB shares ......................................................... 172
What the default administrative shares are ................................................ 173
Share naming considerations ...................................................................... 174
Non-Unicode clients not supported ............................................................ 175
Considerations about directory case-sensitivity when creating shares in a
multiprotocol environment .......................................................................... 175
Elimination of execute permission requirements on share paths ............... 175
Information you need when creating SMB shares ....................................... 176
Creating an SMB share on a CIFS server .................................................... 177
Adding or removing share properties on an existing SMB share ............... 183
Viewing information about SVM shares using the MMC ......................... 186
Commands for managing SMB shares ......................................................... 186

Securing file access by using SMB share ACLs .......................................... 187
Managing SMB share-level ACLs ............................................................... 187
How Data ONTAP uses share-level ACLs .................................................. 188
Creating SMB share access control lists .................................................... 188
Commands for managing SMB share access control lists ......................... 190

Securing file access by using file permissions ............................................ 190
Configuring standard NTFS file permissions by using the Windows
Security tab ................................................................................................. 190

Configuring advanced NTFS file permissions using the Windows
Security tab ................................................................................................. 192
How to configure NTFS file permissions using the Data ONTAP CLI .......... 195
How UNIX file permissions provide access control when accessing files
over SMB ....................................................................................................... 196
Securing file access by using Dynamic Access Control (DAC) ............................. 196
Supported Dynamic Access Control functionality ...................................... 198
Considerations when using Dynamic Access Control and central access policies with CIFS servers .......................................................... 199
Enabling or disabling Dynamic Access Control ......................................... 199
Configuring central access policies to secure data on CIFS servers .......... 200
Displaying information about Dynamic Access Control security .......... 203
Revert considerations for Dynamic Access Control ................................... 204
Where to find additional information about configuring and using
Dynamic Access Control and central access policies ............................ 204

Securing SMB access using export policies ............................................................ 205
How export policies are used with SMB access .......................................... 205
What happens to existing SMB export policies when upgrading ............... 206
Enabling or disabling export policies for SMB access .............................. 207
How export rules work .............................................................................. 208
Examples of export policy rules that restrict or allow access over SMB ... 209
Considerations when reverting export policies for SMB ......................... 211

Managing file access using SMB ............................................................. 212
Using local users and groups for authentication and authorization .......... 212
How Data ONTAP uses local users and groups ........................................ 212
What local privileges are ........................................................................ 216
Requirements and considerations .............................................................. 217
Predefined BUILTIN groups and default privileges .................................. 218
Enabling or disabling local users and groups functionality ....................... 219
Managing local user accounts .................................................................. 221
Managing local groups ............................................................................ 227
Managing local privileges ......................................................................... 234
Configuring bypass traverse checking ....................................................... 237
Allowing users or groups to bypass directory traverse checking ......... 239
Disallowing users or groups from bypassing directory traverse checking .. 240
Displaying information about file security and audit policies ................. 240
Displaying information about file security on NTFS security-style
volumes ...................................................................................................... 242
Displaying information about file security on mixed security-style
volumes ...................................................................................................... 244
Displaying information about file security on UNIX security-style
volumes ...................................................................................................... 246
Displaying information about NTFS audit policies on FlexVol volumes
using the CLI .......................................................................................... 248
Displaying information about NFSv4 audit policies on FlexVol volumes
using the CLI .......................................................................................... 250
Managing NTFS file security, NTFS audit policies, and Storage-Level Access
Guard on SVMs using the CLI .................................................................... 251
Use cases for using the CLI to set file and folder security ...................... 252
Limits when using the CLI to set file and folder security ........................ 252
Requirements for using roaming profiles .......................................................... 311
Configuring roaming profiles ........................................................................... 312
Using folder redirection to store data on a CIFS server ....................................... 312
Requirements for using folder redirection .......................................................... 313
Configuring folder redirection .......................................................................... 313
How to access the ~snapshot directory from Windows clients using SMB 2.x ..... 314
Recovering files and folders using Previous Versions ........................................... 315
Requirements for using Microsoft Previous Versions ........................................... 315
Using the Previous Versions tab to view and manage Snapshot copy data .... 316
Determining whether Snapshot copies are available for Previous
Versions use ........................................................................................................... 316
Creating a Snapshot configuration to enable Previous Versions access ............ 318
Considerations when restoring directories that contain junctions .................... 318

**Deploying CIFS server-based services ............................................................. 319**

Managing home directories .................................................................................. 319
How clustered Data ONTAP enables dynamic home directories ......................... 319
Adding a home directory share ........................................................................... 320
Adding a home directory search path .................................................................. 322
Creating a home directory configuration using the %w and %d variables .... 323
Configuring home directories using the %u variable ............................................ 325
Additional home directory configurations ........................................................... 328
Commands for managing search paths ................................................................. 328
Displaying information about an SMB user's home directory path ................. 329
Managing accessibility to users' home directories .............................................. 329

Configuring SMB client access to UNIX symbolic links .................................... 330
How Data ONTAP enables you to provide SMB client access to UNIX
symbolic links ....................................................................................................... 331
Limits when configuring UNIX symbolic links for SMB access ......................... 332
How to control automatic DFS advertisements in clustered Data ONTAP
with a CIFS server option .................................................................................... 332
Managing whether the CIFS server automatically advertises DFS
capabilities ........................................................................................................... 333
Configuring UNIX symbolic link support on SMB shares ................................. 334
Creating symbolic link mappings for SMB shares ............................................. 335
Commands for managing symbolic link mappings ............................................. 336

Using BranchCache to cache SMB share content at a branch office ................. 336
Requirements, considerations, and recommendations ........................................ 337
Configuring BranchCache ................................................................................... 339
Configuring BranchCache-enabled SMB shares ................................................. 343
Managing and monitoring the BranchCache configuration ................................... 346
Disabling BranchCache on SMB shares ............................................................. 354
Disabling or enabling BranchCache on the SVM ................................................. 356
Deleting the BranchCache configuration on SVMs ............................................ 358
What happens to BranchCache when reverting ............................................... 359
Improving Microsoft remote copy performance ............................................... 359
How ODX works ................................................................................................. 360
Requirements for using ODX ............................................................................. 361
Considerations for using ODX ............................................................................ 362
Use cases for ODX ............................................................................................ 363
Enabling or disabling ODX ................................................................................ 364
Improving client response time by providing SMB automatic node referrals
with Auto Location ............................................................................................. 364
Requirements and considerations when using automatic node referrals .......... 365
Support for automatic node referrals ............................................................... 367
Enabling or disabling SMB automatic node referrals ...................................... 368
Using statistics to monitor automatic node referral activity ........................... 368
How to monitor client-side SMB automatic node referral information
using a Windows client ...................................................................................... 370
Providing folder security on shares with access-based enumeration ............... 370
Enabling or disabling access-based enumeration on SMB shares ................. 371
Enabling or disabling access-based enumeration from a Windows client .... 372
Configuring Data ONTAP for Microsoft Hyper-V and SQL Server
over SMB solutions ............................................................................................ 373
What nondisruptive operations for Hyper-V and SQL Server over SMB means ... 373
Protocols that enable nondisruptive operations over SMB ............................... 374
Key concepts about nondisruptive operations for Hyper-V and SQL
Server over SMB .............................................................................................. 374
How SMB 3.0 functionality supports nondisruptive operations over
SMB shares ....................................................................................................... 376
What the Witness protocol does to enhance transparent failover .................. 376
Share-based backups with Remote VSS ............................................................. 378
Remote VSS concepts ...................................................................................... 378
Example of a directory structure used by Remote VSS ................................. 379
How SnapManager for Hyper-V manages Remote VSS-based backups
for Hyper-V over SMB .................................................................................... 380
How ODX copy offload is used with Hyper-V and SQL Server over SMB
shares ................................................................................................................ 381
Configuration requirements and considerations .............................................. 382
Data ONTAP and licensing requirements ......................................................... 383
Network and data LIF requirements ................................................................. 383
CIFS server and volume requirements for Hyper-V over SMB ........................ 384
CIFS server and volume requirements for SQL Server over SMB ................... 385
Continuously available share requirements and considerations for
Hyper-V over SMB ............................................................................................ 386
Continuously available share requirements and considerations for SQL
Server over SMB ............................................................................................... 387
Remote VSS considerations for Hyper-V over SMB configurations .............. 388
ODX copy offload requirements for SQL Server and Hyper-V over
SMB ................................................................................................................... 389
Recommendations for SQL Server and Hyper-V over SMB configurations ...... 389
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning the Hyper-V or SQL Server over SMB configuration</td>
<td>390</td>
</tr>
<tr>
<td>Completing the volume configuration worksheet</td>
<td>390</td>
</tr>
<tr>
<td>Completing the SMB share configuration worksheet</td>
<td>391</td>
</tr>
<tr>
<td>Creating Data ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server over SMB</td>
<td>393</td>
</tr>
<tr>
<td>Verifying that both Kerberos and NTLMv2 authentication are permitted (Hyper-V over SMB shares)</td>
<td>394</td>
</tr>
<tr>
<td>Verifying that domain accounts map to the default UNIX user</td>
<td>395</td>
</tr>
<tr>
<td>Verifying that the security style of the SVM root volume is set to NTFS</td>
<td>397</td>
</tr>
<tr>
<td>Verifying that required CIFS server options are configured</td>
<td>398</td>
</tr>
<tr>
<td>Verifying that automatic node referrals are disabled</td>
<td>399</td>
</tr>
<tr>
<td>Creating NTFS data volumes</td>
<td>400</td>
</tr>
<tr>
<td>Creating continuously available SMB shares</td>
<td>401</td>
</tr>
<tr>
<td>Adding the SeSecurityPrivilege privilege to the user account (for SQL Server of SMB shares)</td>
<td>402</td>
</tr>
<tr>
<td>Configuring the VSS shadow copy directory depth (for Hyper-V over SMB shares)</td>
<td>402</td>
</tr>
<tr>
<td>Managing Hyper-V and SQL Server over SMB configurations</td>
<td>403</td>
</tr>
<tr>
<td>Configuring existing shares for continuous availability</td>
<td>403</td>
</tr>
<tr>
<td>Enabling or disabling VSS shadow copies for Hyper-V over SMB backups</td>
<td>405</td>
</tr>
<tr>
<td>Considerations for reverting Hyper-V over SMB configurations</td>
<td>406</td>
</tr>
<tr>
<td>Considerations for reverting SQL Server over SMB configurations</td>
<td>407</td>
</tr>
<tr>
<td>Using statistics to monitor Hyper-V and SQL Server over SMB activity</td>
<td>407</td>
</tr>
<tr>
<td>Determining which statistics objects and counters are available</td>
<td>407</td>
</tr>
<tr>
<td>Displaying SMB statistics</td>
<td>409</td>
</tr>
<tr>
<td>Verifying that the configuration is capable of nondisruptive operations</td>
<td>410</td>
</tr>
<tr>
<td>How to use health monitoring to determine whether nondisruptive operation status is healthy</td>
<td>410</td>
</tr>
<tr>
<td>Displaying nondisruptive operation status by using system health monitoring</td>
<td>411</td>
</tr>
<tr>
<td>Verifying the continuously available SMB share configuration</td>
<td>412</td>
</tr>
<tr>
<td>Verifying LIF status</td>
<td>413</td>
</tr>
<tr>
<td>Determining whether SMB sessions are continuously available</td>
<td>415</td>
</tr>
<tr>
<td>Auditing NAS events on SVMs with FlexVol volumes</td>
<td>421</td>
</tr>
<tr>
<td>How auditing works</td>
<td>421</td>
</tr>
<tr>
<td>Basic auditing concepts</td>
<td>421</td>
</tr>
<tr>
<td>How the Data ONTAP auditing process works</td>
<td>422</td>
</tr>
<tr>
<td>Aggregate space considerations when enabling auditing</td>
<td>424</td>
</tr>
<tr>
<td>Auditing requirements and considerations</td>
<td>424</td>
</tr>
<tr>
<td>What the supported audit event log formats are</td>
<td>425</td>
</tr>
<tr>
<td>Viewing audit event logs</td>
<td>425</td>
</tr>
<tr>
<td>How active audit logs are viewed using Event Viewer</td>
<td>426</td>
</tr>
<tr>
<td>SMB events that can be audited</td>
<td>426</td>
</tr>
<tr>
<td>Determining what the complete path to the audited object is</td>
<td>428</td>
</tr>
</tbody>
</table>
Considerations when auditing symlinks and hard links ........................................ 429
Considerations when auditing alternate NTFS data streams ................................ 429
NFS file and directory access events that can be audited ....................................... 431
Planning the auditing configuration ...................................................................... 431
Creating a file and directory auditing configuration on SVMs .............................. 436
   Creating the auditing configuration ............................................................ 436
   Enabling auditing on the SVM ................................................................. 438
   Verifying the auditing configuration ......................................................... 438
Configuring file and folder audit policies ............................................................ 439
   Configuring audit policies on NTFS security-style files and directories ........ 439
   Configuring auditing for UNIX security style files and directories .............. 443
Displaying information about audit policies applied to files and directories ......... 443
   Displaying information about audit policies using the Windows Security tab ................................................................. 443
   Displaying information about NTFS audit policies on FlexVol volumes using the CLI ................................................................. 445
Managing auditing configurations ...................................................................... 447
   Manually rotating the audit event logs ...................................................... 447
   Enabling and disabling auditing on SVMs ................................................ 447
   Displaying information about auditing configurations ............................... 448
   Commands for modifying auditing configurations ...................................... 449
   Deleting an auditing configuration .......................................................... 450
   What the process is when reverting ......................................................... 451
Troubleshooting auditing and staging volume space issues .............................. 451
   How to troubleshoot space issues related to the event log volumes .......... 451
   How to troubleshoot space issues related to the staging volumes (cluster administrators only) ................................................................. 452
Using FPolicy for file monitoring and management on SVMs with
FlexVol volumes .................................................................................................. 453
   How FPolicy works .................................................................................... 453
   What the two parts of the FPolicy solution are ........................................ 453
   What synchronous and asynchronous notifications are ............................. 453
   Roles that cluster components play with FPolicy implementation ............ 454
   How FPolicy works with external FPolicy servers ................................... 455
   What the node-to-external FPolicy server communication process is ........ 456
   How FPolicy services work across SVM namespaces ............................... 458
   FPolicy configuration types ....................................................................... 458
   When to create a native FPolicy configuration ......................................... 459
   When to create a configuration that uses external FPolicy servers .......... 459
   How FPolicy passthrough-read enhances usability for hierarchical storage management ........................................................................................................ 459
   How read requests are managed when FPolicy passthrough-read is enabled ........................................................................................................ 460
   Requirements, considerations, and best practices for configuring FPolicy .... 461
   Ways to configure FPolicy ....................................................................... 461
Requirements for setting up FPolicy ........................................................... 461
Best practices and recommendations when setting up FPolicy ............. 462
Passthrough-read upgrade and revert considerations ............................ 462
What the steps for setting up an FPolicy configuration are ....................... 463
Planning the FPolicy configuration .......................................................... 464
  Planning the FPolicy external engine configuration ............................... 464
  Planning the FPolicy event configuration .............................................. 472
  Planning the FPolicy policy configuration ............................................ 477
  Planning the FPolicy scope configuration ............................................. 482
Creating the FPolicy configuration ......................................................... 485
  Creating the FPolicy external engine ................................................... 486
  Creating the FPolicy event .................................................................. 487
  Creating the FPolicy policy ................................................................. 487
  Creating the FPolicy scope .................................................................. 489
  Enabling the FPolicy policy ................................................................. 489
Modifying FPolicy configurations .......................................................... 490
  Commands for modifying FPolicy configurations .................................. 490
  Enabling or disabling FPolicy policies .................................................. 491
Displaying information about FPolicy configurations ............................. 491
  How the show commands work ............................................................ 492
  Commands for displaying information about FPolicy configurations ..... 492
  Displaying information about FPolicy policy status ............................. 492
  Displaying information about enabled FPolicy policies ......................... 493
Managing FPolicy server connections ..................................................... 494
  Connecting to external FPolicy servers .............................................. 494
  Disconnecting from external FPolicy servers ....................................... 495
  Displaying information about connections to external FPolicy servers ..... 495
  Displaying information about the FPolicy passthrough-read connection
  status .................................................................................................... 497
Copyright information ............................................................................. 499
Trademark information ........................................................................... 500
How to send comments about documentation and receive update
  notifications .......................................................................................... 501
Index ........................................................................................................... 502
Understanding SMB file access with Data ONTAP

There are certain SMB file access concepts you should understand before you configure a CIFS server and then configure SMB shares to let SMB clients access files on your cluster.

How namespaces and volume junctions affect SMB access on SVMs with FlexVol volumes

You must understand what namespaces and volume junctions are and how they work to correctly configure SMB access on Storage Virtual Machines (SVMs) in your storage environment.

Related concepts

Creating and managing data volumes in NAS namespaces on page 148

Related tasks

Configuring character mapping for SMB file name translation on FlexVol volumes on page 161

What namespaces in SVMs with FlexVol volumes are

A namespace is a logical grouping of volumes that are joined together at junction points to create a single, logical file system that derives from the Storage Virtual Machine (SVM) root volume. Each SVM has a namespace.

CIFS and NFS servers on a data SVM can store and access data across the namespace. Each client can access the entire namespace by mounting an export or accessing a single SMB share at the top of the namespace.

Alternatively, SVM administrators can create exports at each volume junction so that clients can create mount points at intermediate locations in the namespace, or they can create SMB shares that point to any directory path in the namespace.

Volumes can be added at any time by mounting them to any location in the namespace. Clients can immediately access the newly added volume, provided that the volume junction is under the point at which they are accessing the namespace and provided that they have sufficient permissions.

Volume junction usage rules

Volume junctions are a way to join individual volumes together into a single, logical namespace to enable data access to NAS clients. Understanding how volume junctions are formed helps you to interpret and apply the usage rules.

When NAS clients access data by traversing a junction, the junction appears to be an ordinary directory. A junction is formed when a volume is mounted to a mount point below the root and is used to create a file-system tree. The top of a file-system tree is always the root volume, which is represented by a slash (/). A junction leads from a directory in one volume to the root directory of another volume.

- Although specifying a junction point is optional when a volume is created, data in the volume cannot be exported (NFS) and a share cannot be created (CIFS) until the volume is mounted to a junction point in the namespace.
- A volume that was not mounted during volume creation can be mounted post-creation.
- New volumes can be added to the namespace at any time by mounting them to a junction point.
• Mounted volumes can be unmounted; however, unmounting a volume disrupts NAS client access to all data in the volume and to all volumes mounted at child junction points beneath the unmounted volume.

• Junction points can be created directly below a parent volume junction, or they can be created on a directory within a volume.
  For example, a path to a volume junction for a volume named “vol3” might be /vol1/vol2/vol3, or it might be /vol1/dir2/vol3, or even /dir1/dir2/vol3.

How volume junctions are used in SMB and NFS namespaces

You can mount volumes at junction points anywhere within the namespace to create a single, logical namespace. If you specify a junction point when the volume is created, the volume is automatically mounted at the time the volume is created and is available for NAS access. You can create SMB shares and NFS exports on the mounted volume.

If you do not specify a junction point, the volume is online but is not mounted for NAS file access. You must mount a volume to a junction point before it can be used for NAS file access.

What the typical NAS namespace architectures are

All Storage Virtual Machine (SVM) name spaces derive from the root volume; however, there are several typical NAS namespace architectures that you can use as you create your SVM name space. You can choose the namespace architecture that matches your business and workflow needs.

The top of the namespace is always the root volume, which is represented by a slash (/). The namespace architecture under the root falls into three basic categories:

• A single branched tree, with only a single junction to the root of the namespace
• Multiple branched trees, with multiple junction points to the root of the namespace
• Multiple stand-alone volumes, each with a separate junction point to the root of the name space

Namespace with single branched tree

An architecture with a single branched tree has a single insertion point to the root of the SVM namespace. The single insertion point can be either a junctioned volume or a directory beneath the root. All other volumes are mounted at junction points beneath the single insertion point (which can be a volume or a directory).
For example, a typical volume junction configuration with the above namespace architecture might look like the following configuration, where all volumes are junctioned below the single insertion point, which is a directory named “data”:

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Volume</th>
<th>Junction</th>
<th>Junction Path</th>
<th>Junction Path Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>corp1</td>
<td>true</td>
<td>/data/dir1/corp1</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>corp2</td>
<td>true</td>
<td>/data/dir1/corp2</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>data1</td>
<td>true</td>
<td>/data/data1</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>eng1</td>
<td>true</td>
<td>/data/data1/eng1</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>eng2</td>
<td>true</td>
<td>/data/data1/eng2</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>sales</td>
<td>true</td>
<td>/data/data1/sales</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>vol11</td>
<td>true</td>
<td>/data/vol11</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>vol12</td>
<td>true</td>
<td>/data/vol12</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>vol13</td>
<td>true</td>
<td>/data/vol13</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>vs1_root</td>
<td>-</td>
<td>/</td>
<td>-</td>
</tr>
</tbody>
</table>

Namespace with multiple branched trees

An architecture with multiple branched trees has multiple insertion points to the root of the SVM namespace. The insertion points can be either junctioned volumes or directories beneath the root. All other volumes are mounted at junction points beneath the insertion points (which can be volumes or directories).
For example, a typical volume junction configuration with the above namespace architecture might look like the following configuration, where there are three insertion points to the root volume of the SVM. Two insertion points are directories named “data” and “projects”. One insertion point is a junctioned volume named “audit”:

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Volume</th>
<th>Junction</th>
<th>Active</th>
<th>Junction Path</th>
<th>Path Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>audit</td>
<td>true</td>
<td>/audit</td>
<td>RW_volume</td>
<td></td>
</tr>
<tr>
<td>vs1</td>
<td>audit_logs1</td>
<td>true</td>
<td>/audit/logs1</td>
<td>RW_volume</td>
<td></td>
</tr>
<tr>
<td>vs1</td>
<td>audit_logs2</td>
<td>true</td>
<td>/audit/logs2</td>
<td>RW_volume</td>
<td></td>
</tr>
<tr>
<td>vs1</td>
<td>audit_logs3</td>
<td>true</td>
<td>/audit/logs3</td>
<td>RW_volume</td>
<td></td>
</tr>
<tr>
<td>vs1</td>
<td>eng</td>
<td>true</td>
<td>/data/eng</td>
<td>RW_volume</td>
<td></td>
</tr>
<tr>
<td>vs1</td>
<td>mktg1</td>
<td>true</td>
<td>/data/mktg1</td>
<td>RW_volume</td>
<td></td>
</tr>
<tr>
<td>vs1</td>
<td>mktg2</td>
<td>true</td>
<td>/data/mktg2</td>
<td>RW_volume</td>
<td></td>
</tr>
<tr>
<td>vs1</td>
<td>project1</td>
<td>true</td>
<td>/projects/project1</td>
<td>RW_volume</td>
<td></td>
</tr>
<tr>
<td>vs1</td>
<td>project2</td>
<td>true</td>
<td>/projects/project2</td>
<td>RW_volume</td>
<td></td>
</tr>
<tr>
<td>vs1</td>
<td>vs1_root</td>
<td>-</td>
<td>/</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

Namespace with multiple stand-alone volumes

In an architecture with stand-alone volumes, every volume has an insertion point to the root of the SVM namespace; however, the volume is not junctioned below another volume. Each volume has a unique path, and is either junctioned directly below the root or is junctioned under a directory below the root.
For example, a typical volume junction configuration with the above namespace architecture might look like the following configuration, where there are five insertion points to the root volume of the SVM, with each insertion point representing a path to one volume.

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Volume</th>
<th>Junction</th>
<th>Junction Path</th>
<th>Path Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>eng</td>
<td>true</td>
<td>/eng</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>mktg</td>
<td>true</td>
<td>/vol/mktg</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>project1</td>
<td>true</td>
<td>/project1</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>project2</td>
<td>true</td>
<td>/project2</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>sales</td>
<td>true</td>
<td>/sales</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>vs1_root</td>
<td>-</td>
<td>/</td>
<td>-</td>
</tr>
</tbody>
</table>

**LIF configuration requirements for file access management**

To properly manage file access control, Data ONTAP must communicate with external services such as NIS, LDAP, and Active Directory servers. The Storage Virtual Machine (SVM) LIFs must be properly configured to allow these communications.

The communication with external services happens over the data LIF of the SVM. Therefore, you must ensure that the SVM has a data LIF properly configured to reach all required external services.

**Related concepts**

Setting up the CIFS server on page 50

**Related information**

Clustered Data ONTAP 8.3 Network Management Guide
How security styles affect data access

Each volume and qtree on the storage system has a security style. The security style determines what type of permissions are used for data on volumes when authorizing users. You must understand what the different security styles are, when and where they are set, how they impact permissions, how they differ between volume types, and more.

Related concepts

Managing how file security is presented to SMB clients for UNIX security-style data on page 75

Related tasks

Configuring security styles on SVM root volumes on page 147
Configuring security styles on FlexVol volumes on page 147
Configuring security styles on qtrees on page 147

What the security styles and their effects are

There are four different security styles: UNIX, NTFS, mixed, and unified. Each security style has a different effect on how permissions are handled for data. You must understand the different effects to ensure that you select the appropriate security style for your purposes.

It is important to understand that security styles do not determine what client types can or cannot access data. Security styles only determine the type of permissions Data ONTAP uses to control data access and what client type can modify these permissions.

For example, if a volume uses UNIX security style, SMB clients can still access data (provided that they properly authenticate and authorize) due to the multiprotocol nature of Data ONTAP. However, Data ONTAP uses UNIX permissions that only UNIX clients can modify using native tools.

<table>
<thead>
<tr>
<th>Security style</th>
<th>Clients that can modify permissions</th>
<th>Permissions that clients can use</th>
<th>Resulting effective security style</th>
<th>Clients that can access files</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNIX</td>
<td>NFS</td>
<td>NFSv3 mode bits</td>
<td>UNIX</td>
<td>NFS and SMB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NFSv4.x ACLs</td>
<td>UNIX</td>
<td></td>
</tr>
<tr>
<td>NTFS</td>
<td>SMB</td>
<td>NTFS ACLs</td>
<td>NTFS</td>
<td></td>
</tr>
<tr>
<td>Mixed</td>
<td>NFS or SMB</td>
<td>NFSv3 mode bits</td>
<td>UNIX</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>NFSv4.x ACLs</td>
<td>UNIX</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>NTFS ACLs</td>
<td>NTFS</td>
<td></td>
</tr>
<tr>
<td>Unified</td>
<td>NFS or SMB</td>
<td>NFSv3 mode bits</td>
<td>UNIX</td>
<td></td>
</tr>
<tr>
<td>(only for Infinite Volumes)</td>
<td></td>
<td>NFSv4.1 ACLs</td>
<td>UNIX</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>NTFS ACLs</td>
<td>NTFS</td>
<td></td>
</tr>
</tbody>
</table>

When the security style is mixed or unified, the effective permissions depend on the client type that last modified the permissions because users set the security style on an individual basis. If the last client that modified permissions was an NFSv3 client, the permissions are UNIX NFSv3 mode bits. If the last client was an NFSv4 client, the permissions are NFSv4 ACLs. If the last client was an SMB client, the permissions are Windows NTFS ACLs.
Note: Data ONTAP initially sets some default file permissions. By default, the effective security style on all data in UNIX, mixed, and unified security style volumes is UNIX and the effective permissions type is UNIX mode bits (0755 unless specified otherwise) until configured by a client as allowed by the default security style. By default, the effective security style on all data in NTFS security style volumes is NTFS and has an ACL allowing full control to everyone.

Related information

Clustered Data ONTAP 8.3 Infinite Volumes Management Guide

Where and when to set security styles

Security styles can be set on FlexVol volumes (both root or data volumes) and qtrees. Security styles can be set manually at the time of creation, inherited automatically, or changed at a later time.

Note: Infinite Volumes always use the unified security style. You cannot configure or change the security style of an Infinite Volume.

How to decide on what security style to use on SVMs with FlexVol volumes

To help you decide what security style to use on a volume, you should consider two factors. The primary factor is the type of administrator that manages the file system. The secondary factor is the type of user or service that accesses the data on the volume.

When you configure the security style on a volume, you should consider the needs of your environment to ensure that you select the best security style and avoid issues with managing permissions. The following considerations can help you decide:

<table>
<thead>
<tr>
<th>Security style</th>
<th>Choose if...</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNIX</td>
<td></td>
</tr>
</tbody>
</table>
|                | • The file system is managed by a UNIX administrator.  
|                | • The majority of users are NFS clients.  
|                | • An application accessing the data uses a UNIX user as the service account.  |
| NTFS           |  
|                | • The file system is managed by a Windows administrator.  
|                | • The majority of users are SMB clients.  
|                | • An application accessing the data uses a Windows user as the service account.  |
| Mixed          |  
|                | The file system is managed by both UNIX and Windows administrators and users consist of both NFS and SMB clients.  |

How security style inheritance works

If you do not specify the security style when creating a new FlexVol volume or qtree, it inherits its security style.

Security styles are inherited in the following manner:

• A FlexVol volume inherits the security style of the root volume of its containing Storage Virtual Machine (SVM).

• A qtree inherits the security style of its containing FlexVol volume.

• A file or directory inherits the security style of its containing FlexVol volume or qtree.
Infinite Volumes cannot inherit security styles. All files and directories in Infinite Volumes always use the unified security style. The security style of an Infinite Volume and the files and directories it contains cannot be changed.

**How authentication provides SMB access security**

Authentication is the process of verifying the identity of an entity. Before users can create SMB connections to access data contained on the Storage Virtual Machine (SVM), they must be authenticated by the domain to which the CIFS server belongs.

The CIFS server supports two authentication methods, Kerberos and NTLM (NTLMv1 or NTLMv2). Kerberos is the default method used to authenticate domain users.

**Related concepts**

- How name mapping is used to secure SMB file access on SVMs with FlexVol volumes on page 23
- How Data ONTAP secures file and directory access on page 24
- Using local users and groups for authentication and authorization on page 212

**Related tasks**

- Setting the CIFS server minimum authentication security level on page 83
- Modifying the CIFS server Kerberos security settings on page 81
- Enabling or disabling AES encryption for Kerberos-based communication on page 84
- Enabling or disabling required password complexity for local SMB users on page 80

**Kerberos authentication**

Data ONTAP supports Kerberos authentication when creating authenticated SMB sessions.

Kerberos is a protocol designed to provide strong authentication within a client/server environment. The basis of the protocol is a shared secret key cryptology system that provides secure authentication in a networked environment.

Kerberos is the primary authentication service for Active Directory. The Kerberos server, or Kerberos Key Distribution Center (KDC) service, stores and retrieves information about security principles in the Active Directory. Unlike the NTLM model, Active Directory clients who want to establish a session with another computer, such as the CIFS server, contact a KDC directly to obtain their session credentials.

**KDC Resource SID Compression feature**

The Key Distribution Center (KDC) can use the Resource SID Compression feature when Active Directory servers are hosted on Windows Server 2012.

Microsoft introduced an enhancement to its Kerberos implementation for Windows Server 2012 that was later called KDC Resource SID Compression, in which the KDC automatically compresses the group security identifiers (SIDs) in the resource domain. This compression can reduce the size of the service ticket and reduce application authentication failures caused by large ticket sizes. To compress resource SIDs, the KDC stores the SID of the resource domain of which the target resource is a member. The KDC inserts only the RID portion of each resource SID into the ResourceGroupIds portion of the authentication data.
NTLM authentication

NTLM client authentication is done using a challenge response protocol based on shared knowledge of a user-specific secret based on a password.

If a user creates an SMB connection using a local Windows user account, authentication is done locally by the CIFS server using NTLMv2.

How name mapping is used to secure SMB file access on SVMs with FlexVol volumes

User mapping between a Windows user and a UNIX user is a fundamental part of multiprotocol access. Multiprotocol access over SMB depends on user mapping between a user’s Windows identity and UNIX identity to evaluate the user’s rights to perform file and folder operations within volumes and qtrees.

Data ONTAP always maps the user’s Windows identity to the user’s UNIX identity during the authentication process. The information about the mapped UNIX user and the UNIX user's groups are saved with the Windows user's credential. Hence, a user credential also contains its mapped UNIX credential.

Data ONTAP maps user names. It does not map groups. However, because group membership is critically important when determining file access, as part of the mapping process the mapped UNIX user’s group membership is retrieved and cached along with the user mapping information.

Related concepts
- How name mapping works on page 23
- How Data ONTAP secures file and directory access on page 24
- Creating name mappings on page 163
- Configuring multidomain name-mapping searches on page 166

Related tasks
- Configuring the default UNIX user on page 99

How name mapping works

Data ONTAP goes through a number of steps when attempting to map user names. They include checking the local name mapping database and LDAP, trying the user name, and using the default user if configured.

When Data ONTAP has to map credentials for a user, it first checks the local name mapping database and LDAP server for an existing mapping. Whether it checks one or both and in which order is determined by the name service configuration of the Storage Virtual Machine (SVM).

- For Windows to UNIX mapping
  If no mapping is found, Data ONTAP checks whether the lowercase Windows user name is a valid user name in the UNIX domain. If this does not work, it uses the default UNIX user provided that it is configured. If the default UNIX user is not configured and Data ONTAP cannot obtain a mapping this way either, mapping fails and an error is returned.

- For UNIX to Windows mapping
  If no mapping is found, Data ONTAP tries to find a Windows account that matches the UNIX name in the CIFS domain. If this does not work, it uses the default CIFS user, provided that it is configured. If the default CIFS user is not configured and Data ONTAP cannot obtain a mapping this way either, mapping fails and an error is returned.
How Data ONTAP secures file and directory access

Data ONTAP evaluates three levels of security to determine whether an entity is authorized to perform a requested action on files and directories residing on the Storage Virtual Machine (SVM). Access is determined by the effective permissions after evaluation of the three security levels.

Types of security layers

Any storage object can contain up to three types of security layers:

- Export (NFS) and share (SMB) security
  Export and share security applies to client accesses to a given NFS export or SMB share. Users with administrative privileges can manage export and share-level security from SMB and NFS clients.

- Storage-Level Access Guard file and directory security
  Storage-Level Access Guard security is applied to SVM volumes. Storage-Level Access Guard applies to all accesses from all NAS protocols to the storage object to which the Storage-Level Access Guard has been applied.
  If you view the security settings on a file or directory from an NFS or SMB client, you will not see the Storage-Level Access Guard security. Storage-Level Access Guard security cannot be revoked from a client, even by a system (Windows or UNIX) administrator.

- NTFS, UNIX, and NFSv4 native file-level security
  Native file-level security exists on the file or directory that represents the storage object. You can set file-level security from a client. File permissions are effective regardless of whether SMB or NFS is used to access the data.

How Data ONTAP uses Storage-Level Access Guard for NFS access

Only NTFS access permissions are supported for Storage-Level Access Guard. For Data ONTAP to perform security checks on UNIX users for access to data on volumes where Storage-Level Access Guard is applied, the UNIX user must map to a Windows user on the SVM that owns the volume.

Storage-Level Access Guard does not apply to SVMs that are UNIX only SVMs and that do not contain CIFS servers.

Related concepts

- How security styles affect data access on page 20
- How name mapping is used to secure SMB file access on SVMs with FlexVol volumes on page 23
- Configuring security styles on page 146
- Creating and configuring SMB shares on page 172
- Securing file access by using SMB share ACLs on page 187
- Securing file access by using file permissions on page 190
- Securing file access by using Storage-Level Access Guard on page 152

Role that export policies play with SMB access

Export policies for SMB access are optional starting with Data ONTAP 8.2, and they are disabled by default. You can enable export policies for SMB if you want to provide an additional layer of SMB access control, in addition to Storage-Level Access Guard and share and file permissions.
Very large CIFS configuration changes might take some time to finish

When you enter CLI commands on the storage system, they are typically executed instantaneously. However, when the CLI command results in a large CIFS configuration change, it might take a while for the configuration change to finish after you entered the CLI command and received confirmation that it was successful.

The larger the change and the more objects are affected, the longer it can take to complete. Examples for this delay are creating several thousand new shares or modifying several thousand share ACLs. The following command areas are affected by this delay:

- Servers
- Home directories
- Shares
- Share ACLs
- Superusers
- Symlink path mapping
- Server security

If you make such very large configuration changes, allow time for the changes to finish.
Configuring and managing Active Directory computer accounts for SVMs (no CIFS license)

You can create and manage an Active Directory (AD) computer account for a Storage Virtual Machine (SVM, formerly known as Vserver) even if you do not have CIFS licensed on any of the cluster nodes. You can also configure and manage preferred domain controllers for the AD computer account.

How to choose whether to create a CIFS server or an Active Directory computer account

You can configure your Storage Virtual Machine (SVM) with a CIFS server that is a member of an Active Directory domain, or if you do not have CIFS licensed, you can create a computer account for your SVM on an Active Directory domain. You need to understand how the configurations differ and how to choose whether you should create a CIFS server or an Active Directory computer account on your SVM.

You can only have one Active Directory account per SVM. Therefore, you must make a choice about whether to create a CIFS server or an Active Directory computer account.

- If you currently have an Active Directory computer account configured on the SVM and you subsequently license CIFS on the cluster and want to create a full-function CIFS server on the SVM, you must first delete the Active Directory computer account.
- If you currently have a CIFS server on the SVM and you subsequently do not need a full CIFS server on the SVM and want to configure an Active Directory computer account instead, you must first delete the CIFS server.

CIFS server

You should choose to create a CIFS server if the following is true:

- You have CIFS licensed on the cluster.
  The CIFS license can be on one or more nodes.
- You want to offer file services and other value-add CIFS functionality, such as home directories or symlink access to SMB clients.

Active Directory computer account

You should choose to create an Active Directory machine account if the following is true:

- You do not have CIFS licensed on the cluster.
- You want to create an Active Directory computer account for the SVM and use it for purposes other than file services or value-add CIFS functionality.
  For example, you might want to use an Active Directory account as the service account for applications accessing data over the iSCSI or FC protocols.

Related concepts

Managing Active Directory computer accounts on page 27
Setting up the CIFS server on page 50
Managing Active Directory computer accounts

You can manage Active Directory computer accounts by creating, displaying information about, or deleting the computer account, changing the domain to which the computer account belongs, and changing or resetting the computer account password.

Related concepts

How to choose whether to create a CIFS server or an Active Directory computer account on page 26
Managing Active Directory computer accounts on page 27
Setting up CIFS servers on page 36

Creating Active Directory computer accounts for SVMs

You can create an Active Directory computer account for your Storage Virtual Machine (SVM) if you want the SVM to have a computer account in the domain, but do not want to license CIFS or do not need to configure SMB file access or CIFS value-add functionality.

Before you begin

- The cluster time must be synchronized to within five minutes of the time on the Active Directory domain controllers for the domain to which you want to associate the SVM computer account. The recommendation is to configure cluster NTP services to use the same NTP servers for time synchronization as the Active Directory domain uses or to use the Active Directory domain controllers as the cluster time servers.
- You must have sufficient permissions to add a computer account to the OU (organizational unit) in the domain to which you want to associate the SVM computer account.
- The SVM must have a data LIF properly configured to reach all required external servers, such as DNS servers and the Active Directory domain controllers.
- DNS must be configured on the SVM, and the DNS servers must either be set to the Active Directory-integrated DNS for the domain to which you want to associate the computer account, or the DNS servers must contain the service location records (SRV) for the domain LDAP and domain controller servers.
- If you want the DNS servers to dynamically register the DNS records for the SVM computer account, the DNS servers must support dynamic DNS.
- If the SVM is configured to use secure DDNS, you must use Active Directory-integrated DNS servers.

About this task

You must keep the following in mind when creating the Active Directory computer account:

- The Active Directory computer account name can be up to 15 characters in length. The following characters are not allowed:

  @ # * ( ) = + [ ] | ; : " , < > \ / ?

- You must use the fully qualified domain name (FQDN) when specifying the domain.
- The default is to add the Active Directory computer account to the CN=Computer object.
You can choose to add the computer account to a different OU by using the optional \(-\text{ou}\) option. When specifying the OU, you do not specify the domain portion of the distinguished name, you only specify the OU or CN portion of the distinguished name. Data ONTAP appends the value provided for the required \(-\text{domain}\) parameter onto the value provided for the \(-\text{ou}\) parameter to produce the Active Directory distinguished name, which is used when creating the Active Directory computer account object.

**Steps**

1. Create the Active Directory computer account:

```
vserver active-directory create -vserver vserver_name -account-name NetBIOS_account_name -domain FQDN [-ou organizational_unit]
```

2. Verify that the Active Directory computer account has been created in the desired OU by using the `vserver active-directory show` command.

**Example**

The following command creates the Active Directory computer account named vs1 for SVM vs1 in the myexample.com domain. The computer account is placed in the OU=eng,DC=myexample,DC=com container.

```
cluster1::> vserver active-directory create -vserver vs1 -account-name vs1 -domain myexample.com -ou OU=eng
```

In order to create an Active Directory machine account, you must supply the name and password of a Windows account with sufficient privileges to add computers to the "OU=eng" container within the "myexample.com" domain.

Enter the user name: Admin_user

Enter the password:

```
cluster1::> vserver active-directory show
```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Account Name</th>
<th>Domain/Workgroup</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>VS1</td>
<td>MYEXAMPLE</td>
</tr>
</tbody>
</table>

**Related concepts**

- How to choose whether to create a CIFS server or an Active Directory computer account on page 26
- Managing domain controller connections for Active Directory computer accounts on page 32

**Changing the Active Directory domain to which the SVM computer account is associated**

You can change the Active Directory domain to which the Storage Virtual Machine (SVM) computer account is associated. This can be useful if you want to use an account from another domain for an application’s service account or if you are migrating SVM resources used by applications to another domain.

**Before you begin**

- The time set on the cluster nodes must match to within five minutes of the time set on the Active Directory domain controllers for the domain to which you want to associate the SVM computer account.
The recommendation is to configure cluster NTP services to use the same NTP servers for time synchronization as the new Active Directory domain uses, or to use the Active Directory domain controllers of the new domain as the cluster time servers.

- You must have sufficient permissions to add a computer account to the OU (organizational unit) in the new domain to which you want to associate the SVM computer account.

- The DNS servers for the SVM must either be set to the Active Directory-integrated DNS for the new domain to which you want to associate the SVM computer account, or the DNS servers must contain the service location records (SRV) for the domain LDAP and domain controller servers.

- If you want the DNS servers to dynamically register the DNS records for the SVM computer account, the DNS servers must support dynamic DNS.

- If the SVM is configured to use secure DDNS, you must use Active Directory-integrated DNS servers.

About this task

- You must use the fully qualified domain name (FQDN) when specifying the domain.

- When changing the domain to which the Active Directory computer account is associated, the computer account in the new domain is placed in the CN=Computers container. You cannot specify where to place the computer account when changing the domain. If you want the location of the computer account to be in a container other than CN=Computers container, you must delete the Active Directory account and re-create it by using the `vserver active-directory create` command.

Steps

1. Change the domain of the Active Directory computer account:

   `vserver active-directory modify -vserver vserver_name -domain FQDN`

2. Verify that the Active Directory computer account has been created in the CN=Computer by using the `vserver active-directory show` command.

Example

The following command changes the domain for the Active Directory computer account named vs1 for SVM vs1 to the example.com domain. The computer account is placed in the CN=Computers container.

```
cluster1::> vserver active-directory modify -vserver vs1 -domain example.com
```

In order to create an Active Directory machine account, you must supply the name and password of a Windows account with sufficient privileges to add computers to the "CN=Computers" container within the "example.com" domain.

Enter the user name: Admin_user

Enter the password:

```
cluster1::> vserver active-directory show
```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Account Name</th>
<th>Domain/Workgroup</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>VS1</td>
<td>EXAMPLE</td>
</tr>
</tbody>
</table>
Displaying information about Active Directory computer accounts for SVMs

You can display information about Active Directory computer accounts for Storage Virtual Machines (SVMs), including the SVM computer account name, the name of the domain to which the computer account is associated, and the organizational unit where the computer account is located.

**Step**

1. Display information about Active Directory computer accounts for SVMs by using the `vserver active-directory show` command.

   You can customize the view by specifying optional parameters. See the man page for the command for details.

**Examples**

The following command displays information about all Active Directory accounts for SVMs on the cluster:

```
cluster1::> vserver active-directory show
```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Account Name</th>
<th>Domain/Workgroup Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>CIFSSERVER1</td>
<td>EXAMPLE</td>
</tr>
<tr>
<td>vs2</td>
<td>CIFSSERVER2</td>
<td>EXAMPLE2</td>
</tr>
</tbody>
</table>

The following command displays detailed information about all Active Directory accounts for SVMs on the cluster:

```
cluster1::> vserver active-directory show -instance
```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Active Directory</th>
<th>NetBIOS Name: CIFSSERVER1</th>
<th>NetBIOS Domain/Workgroup Name: EXAMPLE</th>
<th>Fully Qualified Domain Name: EXAMPLE.COM</th>
<th>Organizational Unit: CN=Computers</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vs2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Deleting Active Directory computer accounts for SVMs

If you no longer want a Storage Virtual Machine (SVM) to have a computer account in an Active Directory domain or if you want to configure a CIFS server on the SVM instead of an Active Directory computer account, you can delete the computer account.

**Before you begin**

You must have sufficient permissions to delete a computer account from the OU (organizational unit) in the Active Directory domain that contains the SVM computer account.

**About this task**

The SVM can have either an Active Directory computer account or a CIFS server, but it cannot have both. If you currently have an Active Directory computer account on your SVM and want to create a
CIFS server on that SVM, you must first delete the Active Directory computer account before you can create the CIFS server.

**Steps**

1. **Delete the Active Directory computer account:**
   
   ```bash
   vserver active-directory delete -vserver vserver_name
   ```
   
   You are asked to enter the user name and password of a user with sufficient permission to delete the computer account from the OU where the computer account is located.

2. **Verify that the computer account is deleted:**

   ```bash
   vserver active-directory show
   ```

**Example**

The following command deletes the Active Directory computer account on SVM vs2:

```
cluster1::> vserver active-directory show

Account     Domain/Workgroup
Vserver        Name        Name
-------------- ----------- ----------------
vs1            VS1         EXAMPLE
vs2            VS2         MYEXAMPLE
```

```
cluster1::> vserver active-directory delete -vserver vs2

In order to delete an Active Directory machine account, you must supply the name and password of a Windows account with sufficient privileges to remove computers from the "example.com" domain.

Enter the user name: Admin_user

Enter the password:

cluster1::> vserver active-directory show

Account     Domain/Workgroup
Vserver        Name        Name
-------------- ----------- ----------------
vs1            VS1         EXAMPLE
```

**Changing or resetting Active Directory computer account passwords for SVMs**

You can change the password for the Active Directory computer account for good security practices, or reset it if the password is lost.

**Step**

1. **Perform one of the following actions:**

<table>
<thead>
<tr>
<th>If you...</th>
<th>Use the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Know the password and want to change it</td>
<td><code>vserver active-directory password-change -vserver vserver_name</code></td>
</tr>
</tbody>
</table>
If you... | Use the command...
---|---
Do not know the password and want to reset it | `vserver active-directory password-reset -vserver vserver_name`

A password reset might be required if the password stored along with the machine account in the Active Directory domain is changed or reset by something other than by the Storage Virtual Machine (SVM). The operation requires the credentials for a user with permission to reset the password in the organizational unit (OU) that contains the computer account.

`-vserver` is the name of the SVM associated with the Active Directory account whose domain password you want to change or reset.

**Managing domain controller connections for Active Directory computer accounts**

You can manage domain controller connections for Active Directory computer accounts by displaying information about discovered Active Directory servers, resetting and rediscovering the Active Directory servers, configuring a list of preferred domain controllers, and displaying the list of preferred domain controllers.

**Related concepts**

*Managing Active Directory computer accounts* on page 27

**Displaying information about discovered Active Directory servers for SVMs**

You can display information related to discovered LDAP servers and domain controllers for the domain to which the Storage Virtual Machine (SVM) computer account is associated.

**About this task**

The `vserver active-directory discovered-servers show` command is an alias of the `vserver cifs domain discovered-servers show` command. You can use either command to display information about discovered Active Directory servers on your SVM.

**Step**

1. To display all or a subset of the information related to discovered servers, enter the following command:

```
vserver active-directory discovered-servers show
```

By default, the command displays the following information about discovered servers:

- Node name
- SVM name
- Active Directory domain name
- Server type
- Preference
- Domain controller name
• Domain controller address
• Status

You can customize the view by specifying optional parameters. See the man page for the command for details.

Example

The following command shows discovered servers for SVM vs1:

```
cluster1::> vserver active-directory discovered-servers show -vserver vs1
```

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Type</th>
<th>Preference</th>
<th>DC-Name</th>
<th>DC-Address</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>example.com</td>
<td>MS-LDAP</td>
<td>adequate</td>
<td>DC-1</td>
<td>192.168.192.24</td>
<td>OK</td>
</tr>
<tr>
<td>example.com</td>
<td>MS-LDAP</td>
<td>adequate</td>
<td>DC-2</td>
<td>192.168.192.25</td>
<td>OK</td>
</tr>
<tr>
<td>example.com</td>
<td>MS-DC</td>
<td>adequate</td>
<td>DC-1</td>
<td>192.168.192.24</td>
<td>OK</td>
</tr>
<tr>
<td>example.com</td>
<td>MS-DC</td>
<td>adequate</td>
<td>DC-2</td>
<td>192.168.192.25</td>
<td>OK</td>
</tr>
</tbody>
</table>

Resetting and rediscovering Active Directory servers

Resetting and rediscovering Active Directory servers on your Storage Virtual Machine (SVM) enables the SVM to discard stored information about LDAP servers and domain controllers. After discarding server information, the SVM reacquires current information about these external servers. This can be useful when the connected servers are not responding appropriately.

About this task

The `vserver active-directory discovered-servers reset-servers` command is an alias of the `vserver cifs domain discovered-servers reset-servers` command. You can use either command to reset and rediscover Active Directory servers on your SVM.

Steps

1. Enter the following command:

   ```
vserver active-directory discovered-servers reset-servers -vserver vserver_name
   ```

2. Display information about the newly rediscovered servers:

   ```
vserver active-directory discovered-servers show -vserver vserver_name
   ```

Example

The following command resets and rediscovers servers for SVM vs1:

```
cluster1::> vserver active-directory discovered-servers reset-servers -vserver vs1
cluster1::> vserver active-directory discovered-servers show
```

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Type</th>
<th>Preference</th>
<th>DC-Name</th>
<th>DC-Address</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>**</td>
<td>NIS</td>
<td>preferred</td>
<td>1.1.3.4</td>
<td>1.1.3.4</td>
<td>OK</td>
</tr>
</tbody>
</table>
Adding or removing preferred domain controllers

Data ONTAP automatically discovers domain controllers through DNS. Optionally, you can add one or more domain controllers to the list of preferred domain controllers on the Storage Virtual Machine (SVM) for the domain in which the Active Directory computer account is configured.

About this task

The `vserver active-directory preferred-dc add` and `vserver active-directory preferred-dc remove` commands are aliases of the `vserver cifs domain preferred-dc add` and `vserver cifs domain preferred-dc remove` commands respectively. You can use either set of commands to manage preferred domain controllers for the Active Directory domain account.

Step

1. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add preferred domain controllers</td>
<td><code>vserver active-directory preferred-dc add -vserver vserver_name -domain domain_name -preferred-dc IP_address, ...</code></td>
</tr>
<tr>
<td>Remove preferred domain controllers</td>
<td><code>vserver active-directory preferred-dc remove -vserver vserver_name -domain domain_name -preferred-dc IP_address, ...</code></td>
</tr>
</tbody>
</table>

`-vserver vserver_name` specifies the SVM name.

`-domain domain_name` specifies the fully qualified name of the domain to which the domain controllers belong.

`-preferred-dc IP_address, ...` specifies one or more IP addresses of the preferred domain controllers to add or remove, as a comma-delimited list. When adding preferred domain controllers, the order of the comma-delimited list indicates order of preference.

Examples

The following command adds domain controller IP addresses 10.1.1.10 and 10.1.1.20 to the list of preferred domain controllers that SVM vs1 uses to manage external access to the example.com domain. The example.com domain contains the SVM Active Directory account.

```
cluster1::> vserver active-directory preferred-dc add -vserver vs1 -domain example.com -preferred-dc 10.1.1.10,10.1.1.20
```

The following command removes the domain controller IP address 10.1.1.20 from the list of preferred domain controllers that Storage Virtual Machine (SVM) vs1 uses to manage external access to the example.com domain.

```
cluster1::> vserver active-directory preferred-dc remove -vserver vs1 -domain example.com -preferred-dc 10.1.1.20
```
Displaying information about preferred domain controllers

You can display information about the list of preferred domain controllers for the domain to which the Active Directory computer account for the Storage Virtual Machine (SVM) is associated. This can be helpful when you want to know which domain controllers are contacted preferentially.

About this task

The `vserver active-directory preferred-dc show` command is an alias of the `vserver cifs domain preferred-dc show` command. You can use either command to display information about preferred domain controllers for the Active Directory domain account.

Step

1. To display all or a subset of the information related to discovered preferred domain controllers, enter the following command:

   ```shell
   vserver active-directory preferred-dc show
   ```

   By default, the command displays the following information about preferred domain controllers:

   - SVM name
   - Active Directory domain name
   - List of IP addresses of the preferred domain controllers

   You can customize the view by specifying optional parameters. See the man page for the command for details.

Example

The following command displays all preferred domain controllers for SVM vs1:

```shell
cluster1::> vserver active-directory preferred-dc show -vserver vs1
Vserver  Domain Name     Preferred Domain Controllers
--------  ---------------  ---------------------------------------------
vs1       example.com     10.1.1.10, 10.1.1.20
```
Setting up CIFS servers

You can enable and configure CIFS servers on Storage Virtual Machines (SVMs) with FlexVol volumes to let SMB clients access files on your cluster.

Each data SVM in the cluster can be bound to exactly one Active Directory domain; however, the data SVMs do not need to be bound to the same domain. Each data SVM can be bound to a unique Active Directory domain.

For information about setting up CIFS servers on SVMs with Infinite Volume, see the Clustered Data ONTAP Infinite Volumes Management Guide.

How to choose whether to create a CIFS server or an Active Directory computer account

You can configure your Storage Virtual Machine (SVM) with a CIFS server that is a member of an Active Directory domain, or if you do not have CIFS licensed, you can create a computer account for your SVM on an Active Directory domain. You need to understand how the configurations differ and how to choose whether you should create a CIFS server or an Active Directory computer account on your SVM.

You can only have one Active Directory account per SVM. Therefore, you must make a choice about whether to create a CIFS server or an Active Directory computer account.

- If you currently have an Active Directory computer account configured on the SVM and you subsequently license CIFS on the cluster and want to create a full-function CIFS server on the SVM, you must first delete the Active Directory computer account.

- If you currently have a CIFS server on the SVM and you subsequently do not need a full CIFS server on the SVM and want to configure an Active Directory computer account instead, you must first delete the CIFS server.

CIFS server

You should choose to create a CIFS server if the following is true:

- You have CIFS licensed on the cluster.
  The CIFS license can be on one or more nodes.

- You want to offer file services and other value-add CIFS functionality, such as home directories or symlink access to SMB clients.

Active Directory computer account

You should choose to create an Active Directory machine account if the following is true:

- You do not have CIFS licensed on the cluster.

- You want to create an Active Directory computer account for the SVM and use it for purposes other than file services or value-add CIFS functionality.
  For example, you might want to use an Active Directory account as the service account for applications accessing data over the iSCSI or FC protocols.

Related concepts

Managing Active Directory computer accounts on page 27

Setting up the CIFS server on page 50
Supported SMB clients and domain controllers

Before you can use SMB with your Storage Virtual Machine (SVM), you need to know which SMB clients and domain controllers Data ONTAP supports.

For the latest information about which SMB clients and domain controllers Data ONTAP supports, see the Interoperability Matrix at mysupport.netapp.com/matrix.

Unsupported Windows features

Before you use CIFS in your network, you need to be aware of certain Windows features that Data ONTAP does not support.

Data ONTAP does not support the following Windows features:

• Encrypted File System (EFS)
• Logging of NT File System (NTFS) events in the change journal
• Microsoft File Replication Service (FRS)
• Microsoft Windows Indexing Service
• Remote storage through Hierarchical Storage Management (HSM)
• Quota management from Windows clients
• Windows quota semantics
• The LMHOSTS file
• NTFS native compression

Prerequisites for CIFS server setup

Certain prerequisites must be met before you begin the CIFS server setup process.

• CIFS must be licensed on the cluster.
• The network to be used to connect the Storage Virtual Machine (SVM) data LIFs to the outside network must be configured (cabled and routing configured).
• You must have a list of IP addresses, the subnet mask, and the default gateway to configure the SVM data LIFs.
• The subnet you use when creating the SVM data LIFs must be routable to all external servers required for services such as Active Directory domain controllers and NIS, DNS, NDMP, and LDAP servers.

  Note: In releases prior to clustered Data ONTAP 8.3, you could use node and cluster management LIFs to contact external servers for the SVM, provided that these LIFs could route to the external servers. Starting with clustered Data ONTAP 8.3, you cannot use node and cluster management LIFs to contact external servers for the SVM.

• If you want the DNS servers to dynamically register the computer account DNS records when you create the CIFS server, the DNS servers must support dynamic DNS.
• If you want to configure secure DDNS, the DNS servers that you configure for the SVM must be Active Directory-integrated DNS servers.
• The administrator creating a CIFS server must belong to the home domain or to a trusted domain.

**Related concepts**

*Setting up the CIFS server* on page 50  
*Managing CIFS servers* on page 70

---

**Planning the CIFS server configuration**

Before you create a CIFS server configuration, you must understand what is involved in each step of the configuration. You must decide what settings you need to use when performing the configuration and record them in the planning worksheets.

You must plan for the following configuration tasks:

• Setting up time services  
• Setting up an IP space, broadcast domain, and subnet  
• Creating the Storage Virtual Machine (SVM) to which you want the CIFS server to belong  
• Setting up networking for the SVM  
• Setting up name services for the SVM  
• Creating the CIFS server

**Related concepts**

*Setting up the CIFS server* on page 50

---

**Information to gather before configuring time services**

Prior to creating a CIFS server, you must configure time services on the cluster. When using Kerberos authentication, the cluster time and the time on the domain controllers of the domain that the CIFS server will join must match to within five minutes; otherwise, CIFS server creation fails. Be sure to record your time server IP addresses.

NTP time services is automatically enabled on the cluster; however, you must specify the IP addresses of the time servers. You can specify up to three time servers.

<table>
<thead>
<tr>
<th>Types of information</th>
<th>Required</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP addresses of the time servers</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Are the cluster time services and the time on the domain controllers of the domain that the CIFS server will join set up so that the time skew between them is always less than five minutes?</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

You should set up time services on the cluster rather than manually adjusting cluster time. This is because, in addition to CIFS server creation failing if the time skew is greater than five minutes, CIFS access to shares hosted on the CIFS server or other CIFS server services that depend on domain authentication fail if the time skew is greater than five minutes when using Kerberos authentication.

The default maximum allowed Kerberos clock skew setting is five minutes. After the CIFS server is set up, you can adjust the maximum allowed settings by using the `vserver cifs security modify` command or by using centralized Active Directory GPOs.

**Related information**

*Clustered Data ONTAP 8.3 System Administration Guide*
Information to gather before creating the IPspace, broadcast domain, and subnet configuration

Before you set up the Storage Virtual Machine (SVM) on which you want to create a CIFS server, you must create an IPspace, broadcast domain, and subnet using values that you determine in advance.

IPspaces, broadcast domains, and subnet configurations provide the network structure within which SVMs reside.

- An IPspace defines a distinct IP address space within the cluster and is a way to allocate a separate network space to provide secure administration and routing for SVMs.

- A broadcast domain groups ports that belong in the same Layer 2 network and sets the MTU for the broadcast domain ports. Broadcast domains are assigned to an IPspace. An IP space can contain one or more broadcast domains.

- A subnet contains specific pools of IP addresses and a default gateway that can be assigned to LIFs used by SVMs residing within the IPspace.

Information to gather to create the IPspace

When setting up a CIFS server, you can create a new IPspace or you can use the Default IPspace or any other existing IPspace.

<table>
<thead>
<tr>
<th>Types of information</th>
<th>Required</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPspace name</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>• The name to assign to the IPspace.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• The IPspace name must be unique within the cluster.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Information to gather to create the broadcast domain

- When you create a broadcast domain, Data ONTAP automatically creates a failover group with the same name.

- The failover group contains all the ports assigned to that broadcast domain.

- If desired, you can use an existing broadcast domain within an existing IPspace when creating an SVM for the CIFS server (including the Default broadcast domain in the Default IPspace).

<table>
<thead>
<tr>
<th>Types of information</th>
<th>Required</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPspace name</td>
<td></td>
<td>No (if using the Default IPspace)</td>
</tr>
<tr>
<td>• The IPspace to which the broadcast domain is assigned.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• The IPspace must exist.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• If not specified, the broadcast domain is assigned to the Default IPspace.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| Broadcast domain name  |          | Yes         |
| • The name to assign to the broadcast domain. |          |             |
| • The name must be unique within the IPspace. |          |             |</p>
<table>
<thead>
<tr>
<th>Types of information</th>
<th>Required</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MTU</strong></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>- The MTU of the broadcast domain.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- You can specify either 1500 or 9000.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- The MTU value is applied to all ports in the broadcast domain and to any ports that are later added to the broadcast domain.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> The MTU value must match all the devices connected to that network.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Ports</strong></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>- The network ports to add to the broadcast domain.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- The ports assigned to the broadcast domain can be physical ports, VLANs, or interface groups (ifgroups). For more information about setting up VLANs or interface groups, see the <em>Clustered Data ONTAP Network Management Guide</em>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- If a port is in another broadcast domain, it must be removed before it can be added to the broadcast domain.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Ports are assigned by specifying both the node name and port: for example, “node1:e0d”.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- The default is to not assign any ports. Ports can be added to the broadcast domain at any time.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Information to gather to create the subnet

- When creating a LIF on the SVM, you can specify the name of the subnet instead of supplying an IP address and a subnet.

- Since a subnet can be configured with a default gateway, you do not have to create the default gateway in a separate step when creating an SVM.

- A broadcast domain can contain one or more subnets. You can configure SVM LIFs that are on different subnets by associating more than one subnet with the IPspace's broadcast domain.

- Each subnet must contain IP addresses that do not overlap with IP addresses assigned to other subnets within the same IPspace.

- If desired, you can use any existing subnet within the desired IPspace when creating your CIFS server.

- If desired, you can assigned specific IP addresses to SVM data LIFs and create a default gateway for the SVM instead of using a subnet. For more information about using this method to assign IP addresses to data LIFs, see the *Clustered Data ONTAP Network Management Guide*. 
### Types of information

<table>
<thead>
<tr>
<th><strong>IPspace name</strong></th>
<th>Required</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The name of an existing IPspace to which the subnet will be assigned.</td>
<td>No</td>
<td>(if using the Default IPspace)</td>
</tr>
<tr>
<td>• If not specified, the subnet is assigned to the Default IPspace.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Subnet name</strong></th>
<th>Required</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The name of the subnet to be created.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>• The name must be unique within the IPspace to which it is assigned.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Broadcast domain name</strong></th>
<th>Required</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The name of the broadcast domain to which the subnet will be assigned.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>• The broadcast domain must reside in the specified IPspace.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Subnet name and mask</strong></th>
<th>Required</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>The subnet address and mask within which the IP addresses reside.</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Gateway</strong></th>
<th>Required</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>• You can specify a default gateway for the subnet.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>• If you do not assign a gateway when you create the subnet, you can assign one to the subnet at any time.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>IP address ranges</strong></th>
<th>Required</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>• You can specify a range or specific IP addresses within the subnet. For example, you can specify a range such as “192.168.1.1-192.168.1.100, 192.168.1.112, 192.168.1.145”.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>• If you do not specify an IP address range, the entire range of IP addresses within the specified subnet are available to assign to LIFs.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Force update of LIF associations</strong></th>
<th>Required</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Specifies whether to force the update of existing LIF associations.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>• By default, subnet creation fails if any service processor interfaces or network interfaces are using the IP addresses in the ranges provided.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Using this parameter associates any manually addressed interfaces with the subnet and allows the command to succeed.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Related information

Clustered Data ONTAP 8.3 Network Management Guide
Information to gather before configuring the SVM

Prior to creating the CIFS server, you must configure the Storage Virtual Machine (SVM) using values that you determine in advance. You must record values for the SVM name, the root volume name and security style, the name of the aggregate on which to create the root volume, the IPspace, and other optional settings.

The values that you record are for creating an SVM with FlexVol volumes. For information about creating an SVM with Infinite Volume, see the Clustered Data ONTAP Infinite Volumes Management Guide.

The values that you record are for creating a default data SVM. If you are creating a MetroCluster source SVM, see the Clustered Data ONTAP System Administration Guide for Cluster Administrators.

<table>
<thead>
<tr>
<th>Types of information</th>
<th>Required</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SVM name</strong></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>• Specifies the name you want to assign to the SVM.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• The SVM name can contain alphanumeric characters and the following three special characters: . (period), - (hyphen), and _ (underscore).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• The name of the SVM should not start with a number or either of the following special characters: . (period) or - (underscore).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• The maximum number of characters allowed in the SVM name is 47.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• You should use a fully qualified domain name (FQDN) to ensure unique SVM names across cluster leagues.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Root volume name</strong></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>• Specifies the name for the SVM root volume.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• The root volume name must start with an alphabetic character (a to z or A to Z) and be 203 or fewer characters long.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Aggregate name</strong></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>• Specifies the name of the aggregate that holds the SVM root volume.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• The aggregate must exist.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Security style</strong></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>• Specifies the security style for the SVM root volume.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Possible values are ntfs, unix, and mixed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Types of information</td>
<td>Required</td>
<td>Your values</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>IPspace</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Specifies the name of the IPspace to which the SVM is assigned.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>• If an IPspace is not specified, the SVM is assigned to the Default IPspace that is automatically created by Data ONTAP.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>• The IPspace must exist.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SVM language setting</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Specifies the default language to use for the SVM and its volumes.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>• If you do not specify a default language, the default SVM language is set to C.UTF-8.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>• The SVM language setting determines the character set used to display file names and data for all NAS volumes in the SVM. The language of the SVM with FlexVol volumes can be modified after the SVM is created. For more information about setting the SVM language, see the <em>Clustered Data ONTAP System Administration Guide for Cluster Administrators</em>.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td><strong>Snapshot policy</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Specifies the Snapshot policy to apply to the SVM. If you do not specify a Snapshot policy, the default cluster Snapshot policy is applied to the SVM.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>• The Snapshot policy is enabled by default. By default, the Snapshot policy is inherited by the volumes on the SVM. You can change which Snapshot policy is applied to the SVM at any time.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>See the Snapshot copy section of the <em>Clustered Data ONTAP Logical Storage Management Guide</em> for more information about Snapshot policies.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td><strong>Quota policy</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Specifies the quota policy to apply to the SVM. If you do not specify a quota policy, a blank quota policy named “default” is created and applied to the SVM.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>• By default, the quota policy is inherited by the volumes on the SVM.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>• You can change which quota policy is applied to the SVM at any time.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>• This setting is supported only on SVMs with FlexVol volumes.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>See the quota section of the <em>Clustered Data ONTAP Logical Storage Management Guide</em> for more information about quotas.</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
Information to gather before creating data LIFs on the SVM

Prior to setting up the CIFS server, you must create data LIFs for the Storage Virtual Machine (SVM) using the values that you determine in advance. You must record the SVM name and the values for the LIF name, the LIF role, protocols allowed, home node and port for the LIF, and subnet name.

You can also use IP addresses and default gateways instead of subnets when creating LIFs. For more information, see the Clustered Data ONTAP Network Management Guide.

<table>
<thead>
<tr>
<th>Types of information</th>
<th>Required</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SVM name</strong></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Specifies the name of the SVM on which to create the data LIFs.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Data LIF names</strong></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Specifies the name to give to the logical network interfaces that clients use when accessing data on the SVM.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>You can assign multiple data LIFs per node, and you can assign LIFs to any node in the cluster, provided that the node has available data ports.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>To provide redundancy, you should create at least two data LIFs for each data subnet, and the LIFs assigned to a particular subnet should be assigned home ports on different nodes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Important:</strong> If you are configuring the CIFS server to host Hyper-V or SQL Server over SMB for nondisruptive operation solutions, the Storage Virtual Machine (SVM) must have at least one data LIF on every node in the cluster.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>You can provide descriptive names for the interfaces. For example, you can name the data LIFs according to the node assigned as their home node. For example, you can name a LIF whose home node is node1 “lif1”, a LIF whose home node is node2 “lif2”, and so on.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>You should record a LIF name for each data LIF.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>LIF role</strong></td>
<td>Yes</td>
<td>data</td>
</tr>
<tr>
<td>Specifies the role of the LIF.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data LIFs are assigned the data role.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Types of information

<table>
<thead>
<tr>
<th>Types of information</th>
<th>Required</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allowed protocols</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Specifies the protocols that can use the data LIFs (CIFS, NFS, FlexCache, iSCSI, FC, and none).</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>• By default, CIFS, NFS, and FlexCache are allowed. The FlexCache protocol enables a volume to be used as an origin volume for a FlexCache volume on a system running Data ONTAP operating in 7-mode.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> Protocols that can use the LIF cannot be modified after the LIF is created. If you might want to allow other protocols on the data LIF at a future time, you should configure the LIF to allow those protocols during LIF creation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Data LIF home node</strong></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>• The home node is the node to which the logical interface returns when the LIF is reverted to its home port.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>You should record a home node for each data LIF.</td>
<td></td>
</tr>
<tr>
<td><strong>Data LIF home port</strong></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>• The home port is the port to which the logical interface returns when the LIF is reverted to its home port.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>You should record a home port for each data LIF.</td>
<td></td>
</tr>
<tr>
<td><strong>Subnet name</strong></td>
<td></td>
<td>Yes (if using a subnet to assign network information to the data LIFs)</td>
</tr>
<tr>
<td>• The name of the subnet to assign to the SVM.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>All data LIFs used to create continuously available SMB connections to application servers must be on the same subnet.</td>
<td></td>
</tr>
</tbody>
</table>

### Related information

*Clustered Data ONTAP 8.3 Network Management Guide*

### Information to gather before configuring name services

Prior to creating a CIFS server, you must configure DNS name services using values that you determine in advance. Optionally, you can configure which sources to use for each name service and the order in which to look up information in the name service databases. Optionally, you can configure NIS or LDAP name services.

### Information for configuring the ordering of name services in the name services database (optional)

Storage Virtual Machines (SVMs) use the name services (nsswitch) database to determine the order in which to look up the name service sources for a given name service. You can use the default configuration or you can customize the ordering of name services.

The database table stores a separate name service list for each of the following database types:
<table>
<thead>
<tr>
<th>Database type</th>
<th>Defines name service sources for...</th>
<th>Valid sources are...</th>
<th>Defaults for each name service are...</th>
</tr>
</thead>
<tbody>
<tr>
<td>hosts</td>
<td>Converting host names to IP addresses</td>
<td>files, dns</td>
<td>files, dns</td>
</tr>
<tr>
<td>group</td>
<td>Looking up user group information</td>
<td>files, nis, ldap</td>
<td>files</td>
</tr>
<tr>
<td>passwd</td>
<td>Looking up user information</td>
<td>files, nis, ldap</td>
<td>files</td>
</tr>
<tr>
<td>netgroup</td>
<td>Looking up netgroup information</td>
<td>files, nis, ldap</td>
<td>files</td>
</tr>
<tr>
<td>namemap</td>
<td>Mapping user names</td>
<td>files, ldap</td>
<td>files</td>
</tr>
</tbody>
</table>

If you want to use the default settings, you do not need to do any additional configuration for the ordering of name services databases. If you want to use nondefault values, you should enter the desired values:

<table>
<thead>
<tr>
<th>Name service</th>
<th>Use default?</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Passwd</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Netgroup</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Namemap</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** If you are configuring NIS or LDAP name services, you must configure the appropriate name service databases to use the desired name service with the desired ordering.

### Information for configuring DNS

You must configure DNS on the SVM before creating a CIFS server.

<table>
<thead>
<tr>
<th>Types of information</th>
<th>Required</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SVM name</strong></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Specifies the name of the SVM on which you want to create a CIFS server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DNS domain name</strong></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>• Specifies a list of domain names to append to a host name when performing host-to-IP name resolution.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• List the local domain first, followed by the domain names for which DNS queries are most often made.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Types of information**

**IP addresses of the DNS servers**

- List of IP addresses for the DNS servers that will provide name resolution for the CIFS server.

- The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.

  The SRV record is used to map the name of a service to the DNS computer name of a server that offers that service. CIFS server creation fails if Data ONTAP cannot obtain the service location records through local DNS queries.

  The simplest way to ensure that Data ONTAP can locate the Active Directory SRV records is to configure Active Directory-integrated DNS servers as the SVM DNS servers.

  You can use non-Active Directory-integrated DNS servers provided that the DNS administrator has manually added the SRV records to the DNS zone that contains information about the Active Directory domain controllers.

- For information about the Active Directory-integrated SRV records, see the topic *How DNS Support for Active Directory Works* on Microsoft TechNet.

  *Microsoft TechNet: How DNS Support for Active Directory Works*

See the man page for the command to find information about other optional parameter settings.

**Information for configuring dynamic DNS on the SVM**

Before you can use dynamic DNS to automatically adding DNS entries to your Active Directory-integrated DNS servers, you must dynamic DNS (DDNS) on your SVM. You configure DDNS on the SVM before you configure the CIFS server. DNS records will be created for every data LIF on the SVM. By creating multiple data LIFS on the SVM, you can load balance client connections to the assigned data IP addresses. DNS load balances connections that are made using the host name to the assigned IP addresses in a round-robin fashion.

<table>
<thead>
<tr>
<th>Types of information</th>
<th>Required</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SVM name</strong></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Specifies the name of the SVM on which you want to create a CIFS server.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Whether to use DDNS</th>
<th>Yes (if enabling)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies whether to use DDNS.</td>
<td></td>
</tr>
<tr>
<td>The DNS servers configured on the SVM must support DDNS. By default DDNS is disabled.</td>
<td></td>
</tr>
</tbody>
</table>
Types of information | Required | Your values
---|---|---
**Whether to use secure DDNS**
- Secure DDNS is supported only with Active Directory-integrated DNS.
- If your Active Directory-integrated DNS allows only secure DDNS updates, the value for this parameter must be `true`.
- By default, secure DDNS is disabled.

**FQDN of the DNS domain**
- Specifies the FQDN of the DNS domain.
- You must use the same domain name configured for DNS name services on the SVM.

**Information for configuring NIS (optional)**
- If you specified NIS as a name service option when you configured the name services databases, you should create a NIS domain configuration for the SVM.
- If you rely on NIS for retrieving information about UNIX user and group information or for successful Windows-to-UNIX user name mapping, you must configure NIS for SMB access to succeed.
- If you use the default UNIX user for all name mapping, you might not need to configure NIS for this SVM.

Types of information | Required | Your values
---|---|---
*SVM name*
The name of the SVM on which to configure NIS. | Yes |
*NIS domain name*
- The NIS domain name for which a configuration is created.
- The maximum NIS domain name length is 64 characters. | Yes |
*IP addresses of the NIS servers*
- List of IP addresses for the NIS servers.
- You can specify multiple NIS servers as a comma-delimited list. | Yes |
*Is the NIS configuration active?*
- Specifies whether the NIS domain configuration is active.
- A SVM can have multiple NIS domain configurations, but only one of the configurations can be active at a given time. | Yes |

You can find information about configuring LDAP on the SVM in the *Clustered Data ONTAP File Access Management Guide for NFS*.
Information to gather before creating the CIFS server

Prior to creating the CIFS server, you must decide upon information such as the name of the Storage Virtual Machine (SVM) on which to create the CIFS server, the name of the CIFS server and the domain that it will join, and optionally, the OU for the computer object, a comment, and the names of NetBIOS aliases.

The described values are based on the assumption that you are creating a CIFS server on a default data SVM. If you are creating a CIFS server on a MetroCluster source SVM, see the MetroCluster Installation and Configuration Guide.

<table>
<thead>
<tr>
<th>Types of information</th>
<th>Required</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SVM name</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The name of the SVM you created to host the CIFS server</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><strong>CIFS server name</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• The name of the CIFS server.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>• The CIFS server name can be the same as or different from the SVM name.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• The CIFS server name can be up to 15 characters. Characters that are not allowed include the following characters: @ * ( ) = + [ ]</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>: &quot; , &lt; &gt; / ?</td>
<td></td>
</tr>
<tr>
<td><strong>Domain name</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• The FQDN of the Active Directory domain that you want the CIFS server to join.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>• A CIFS server appears as a member Windows server object in the Active Directory store.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>OU (Organizational unit )</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• The OU within the Active Directory domain where you want the CIFS server computer object placed.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>• By default, the CIFS server computer object storage location is CN=Computers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Comment</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• A descriptive text comment for the CIFS server that can be up to 256 characters long.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>• SMB clients can see the CIFS server comment when browsing servers on the network.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• If there is a space in the comment, you must enclose the entire string in quotation marks.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Types of information

<table>
<thead>
<tr>
<th>Types of information</th>
<th>Required</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetBIOS Aliases</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

- A comma-delimited list of one or more NetBIOS aliases, which are alternate names for the CIFS server.
- You can configure up to 200 NetBIOS aliases on the CIFS server.
- The NetBIOS alias name can be up to 15 characters.
- Characters that are not allowed include the following characters:
  @ # * ( ) = + [ ] | ; : " , < > / ?

Data ONTAP attempts to identify the default site to associate with the CIFS server. If Data ONTAP cannot determine the appropriate site for the CIFS server, you can specify a default site when you create the CIFS server. By default, the initial administrative status of the newly created CIFS server is up. When you create the CIFS server, you can specify that the initial status of the CIFS server is down. See the man pages for the 
vserver cifs create
command for more information.

Related information

Clustered Data ONTAP 8.3.1 man page: vserver cifs create - Create a CIFS server
Clustered Data ONTAP 8.3 MetroCluster Installation and Configuration Guide

Setting up the CIFS server

Setting up the CIFS server involves completing the CIFS server configuration worksheet, creating the Storage Virtual Machine (SVM) with the proper setting for CIFS access, configuring DNS on the SVM, creating the CIFS server, and, if necessary, setting up UNIX user and group name services.

Before you set up your CIFS server, you must understand the choices you need to make when performing the setup. You should make decisions regarding the SVM, DNS, and CIFS server configurations and record your choices in the planning worksheet prior to creating the configuration. This can help you in successfully creating a CIFS server.

Creating SVMs can only be completed by a cluster administrator.

Steps

1. Configuring time services (cluster administrators only) on page 52
   You must ensure that the cluster time and the time on the domain controllers of the domain to which the CIFS server will belong matches to within five minutes. You should configure time services on the cluster prior to creating the CIFS server.

2. Creating an IPspace for the SVM (cluster administrators only) on page 52
   Before you can create the Storage Virtual Machine (SVM) on which you want to create the CIFS server, you must configure the IPspace that will contain the SVM. IPspaces are distinct IP address spaces used to secure storage, administration, and routing.

3. Determining which ports can be used for a new broadcast domain (cluster administrators only) on page 53
   Before you can configure a broadcast domain to add to the new IPspace, you must determine what ports are available and can be used for a new broadcast domain.

4. Removing ports from an existing broadcast domain prior to adding them to the new broadcast domain (cluster administrators only) on page 55
If the ports that you want to add to the new broadcast domain are already in another broadcast domain, you must remove the ports from that broadcast domain before assigning them to the new broadcast domain.

5. Creating a broadcast domain for the IPspace (cluster administrators only) on page 56
   You must create a broadcast domain for the IPspace. A broadcast domain defines what network ports are grouped into the same Layer 2 network. The ports in a network domain can be used by the Storage Virtual Machines (SVMs) assigned to that IPspace.

6. Creating a subnet for the IPspace (cluster administrators only) on page 57
   After you create the broadcast domain, you should create a subnet to allocate specific blocks of IPv4 or IPv6 addresses to be used later when you create LIFs for the Storage Virtual Machine (SVM). This enables you to create LIFs more easily by specifying a subnet name instead of having to specify IP address and network mask values for each LIF.

7. Creating an SVM with FlexVol volumes for the CIFS server (cluster administrators only) on page 59
   Prior to creating a CIFS server, you must create a Storage Virtual Machine (SVM) with a configuration that is appropriate for hosting the CIFS server.

8. Creating LIFs on the SVM (cluster administrators only) on page 61
   Before you can provide SMB access to the CIFS server, you must create LIFs on the Storage Virtual Machine (SVM). The LIFs that you create must be routable to all external servers required for services such as Active Directory (AD) domain controllers, DNS, NIS, LDAP, and NDMP.

9. Configuring DNS services for the SVM on page 63
   You must configure DNS services for the Storage Virtual Machine (SVM) before creating the CIFS server. Generally, the DNS name servers are the Active Directory-integrated DNS servers for the domain that the CIFS server will join.

10. Configuring dynamic DNS on the SVM on page 64
    If you want the Active Directory-integrated DNS server to dynamically register the CIFS server's DNS records in DNS, you must configure dynamic DNS (DDNS) on the Storage Virtual Machine (SVM) before creating the CIFS server.

11. Creating a CIFS server on page 65
    A CIFS server is necessary to provide SMB clients with access to the Storage Virtual Machine (SVM). After you set up DNS services on the SVM, you can create a CIFS server.

12. Configuring NIS or LDAP name services on the SVM on page 67
    With SMB access, user mapping to a UNIX user is always performed, even if accessing data in an NTFS security-style volume. If you map Windows users to corresponding UNIX users whose information is stored in NIS or LDAP directory stores or if you use LDAP for name mapping, you should configure these name services during CIFS setup.

Related concepts

- Prerequisites for CIFS server setup on page 37
- Planning the CIFS server configuration on page 38
- Managing CIFS servers on page 70

Related information

- Clustered Data ONTAP 8.3 System Administration Guide
- Clustered Data ONTAP 8.3 Network Management Guide
Configuring time services (cluster administrators only)

You must ensure that the cluster time and the time on the domain controllers of the domain to which the CIFS server will belong matches to within five minutes. You should configure time services on the cluster prior to creating the CIFS server.

About this task

Steps

1. Configure time services by using the `cluster time-service ntp server create` command.

   Example
   
   ```
   cluster time-service ntp server create -server 10.10.10.1
   cluster time-service ntp server create -server 10.10.10.2
   ```

2. Verify that time services are set up correctly by using the `cluster time-service ntp server show` command.

   Example
   
   ```
   cluster time-service ntp server show
   ```

<table>
<thead>
<tr>
<th>Server</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.1</td>
<td>auto</td>
</tr>
<tr>
<td>10.10.10.2</td>
<td>auto</td>
</tr>
</tbody>
</table>

Related references

*Information to gather before configuring time services* on page 38

Creating an IPspace for the SVM (cluster administrators only)

Before you can create the Storage Virtual Machine (SVM) on which you want to create the CIFS server, you must configure the IPspace that will contain the SVM. IPspaces are distinct IP address spaces used to secure storage, administration, and routing.

About this task

If you already have an IPspace configured to which you want to assign the SVM, you can use that IPspace instead of configuring a new one.

Step

1. Create an IPspace by using the `network ipspace create` command.

   Example
   
   ```
   network ipspace create -ipspace ipspace1
   ```

   ```
   network ipspace show
   ```

<table>
<thead>
<tr>
<th>IPspace</th>
<th>Vserver List</th>
<th>Broadcast Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The IPspace is created, along with the system SVM for that IPspace. The system SVM carries management traffic.

**After you finish**

You must configure a broadcast domain for the IPspace.

- You must determine which ports you want to add to the broadcast domain.
- If the ports are currently assigned to another broadcast domain, you must remove them from that broadcast domain so that they are unassigned and available to add to the new broadcast domain.
- You can then create a new broadcast domain and add the ports to it.

**Related references**

*Information to gather before creating the IPspace, broadcast domain, and subnet configuration* on page 39

**Determining which ports can be used for a new broadcast domain (cluster administrators only)**

Before you can configure a broadcast domain to add to the new IPspace, you must determine what ports are available and can be used for a new broadcast domain.

**Before you begin**

All existing LIFs are located on their home ports.

**About this task**

- By default, ports are assigned to either the Cluster IPspace or the Default IPspace.
  - The Cluster IPspace contains the Cluster broadcast domain, which is the container for the ports assigned as cluster ports.
  - The Default IPspace contains the Default broadcast domain, which is the default container for ports, subnets, and Storage Virtual Machines (SVMs) that serve data.
    - The Default IPspace also contains the ports assigned to the cluster management and node management LIFs.
    - As the default container for noncluster ports, unused ports in the Default IPspace are available for a new broadcast domain.
- Ports can be physical ports, VLANs, or interface groups (a logical grouping of interface ports) also known as *ifgroups.*
  This CIFS server setup workflow uses physical ports. For more information about configuring VLANs or interface groups, see the *Clustered Data ONTAP Network Management Guide* or the man pages for the `network port ifgrp` and `network port vlan` command families.
- The ports that you want to add to the new broadcast domain cannot be assigned to an existing broadcast domain.
• If the ports that you want to add to the broadcast domain are already in another broadcast domain (for example, the Default broadcast domain in the Default IPspace), you must remove the ports from that broadcast domain before assigning them to the new broadcast domain.

• Ports that have LIFs assigned to them cannot be removed from a broadcast domain.

• Because the cluster management and node management LIFs are assigned to the Default broadcast domain in the Default IPspace, the ports assigned to these LIFs cannot be removed from the Default broadcast domain.

Steps

1. Determine what the current port assignments are by using the `network port show` command.

Example

```
network port show
```

<table>
<thead>
<tr>
<th>Node</th>
<th>Port</th>
<th>IPspace</th>
<th>Broadcast Domain</th>
<th>Link</th>
<th>MTU</th>
<th>Admin/Oper</th>
</tr>
</thead>
<tbody>
<tr>
<td>node1</td>
<td>e0a</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0b</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0c</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0d</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0e</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0f</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0g</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td>node2</td>
<td>e0a</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0b</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0c</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0d</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0e</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0f</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0g</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
</tbody>
</table>

In this example, the output from the command provides the following information:

• Ports `e0c, e0d, e0e, e0f, and e0g` on each node are assigned to the Default broadcast domain.

• These ports are potentially available to use in the broadcast domain of the IPspace that you want to create.

2. Determine which of the ports in the Default broadcast domain are assigned to LIF interfaces and, therefore, cannot be moved to a new broadcast domain by using the `network interface show` command.

Example

```
network interface show
```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Logical Interface</th>
<th>Status</th>
<th>Network Address/Mask</th>
<th>Current Node</th>
<th>Current Is Port</th>
<th>Home</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster</td>
<td>node1_clus1</td>
<td>up/up</td>
<td>10.0.2.40/24</td>
<td>node1</td>
<td>e0a</td>
<td>true</td>
</tr>
<tr>
<td></td>
<td>node1_clus2</td>
<td>up/up</td>
<td>10.0.2.41/24</td>
<td>node1</td>
<td>e0b</td>
<td>true</td>
</tr>
<tr>
<td></td>
<td>node2_clus1</td>
<td>up/up</td>
<td>10.0.2.42/24</td>
<td>node2</td>
<td>e0a</td>
<td>true</td>
</tr>
<tr>
<td></td>
<td>node2_clus2</td>
<td>up/up</td>
<td>10.0.2.43/24</td>
<td>node2</td>
<td>e0b</td>
<td>true</td>
</tr>
</tbody>
</table>
In this example, the output from the command provides the following information:

- The node ports are assigned to port e0c on each node and the cluster administrative LIFs home node is on e0c on node1.
- Ports e0d, e0e, e0f, and e0g on each node are not hosting LIFs and can be removed from the Default broadcast domain and then added to a new broadcast domain for the new IPspace.

**After you finish**

Use the information obtained in this task to remove the ports from the existing broadcast domain in preparation for creating your new broadcast domain.

**Related references**

*Information to gather before creating the IPSpace, broadcast domain, and subnet configuration* on page 39

**Removing ports from an existing broadcast domain prior to adding them to the new broadcast domain (cluster administrators only)**

If the ports that you want to add to the new broadcast domain are already in another broadcast domain, you must remove the ports from that broadcast domain before assigning them to the new broadcast domain.

**Before you begin**

You must already know which ports are available for removal from the existing broadcast domain.

**Steps**

1. Remove the ports to be assigned to the new broadcast domain from the Default broadcast domain by using the `network port broadcast-domain remove-ports` command.

   **Example**

   ```
   network port broadcast-domain remove-ports --ipspace Default --broadcast-domain Default --ports node1:e0d,node1:e0e,node2:e0d,node2:e0e
   ```

2. Verify that the ports are not assigned to a broadcast domain by using the `network port show` command.

   **Example**

   ```
   network port show
   ```

---

<table>
<thead>
<tr>
<th>Node</th>
<th>Port</th>
<th>IPspace</th>
<th>Broadcast Domain</th>
<th>Link</th>
<th>MTU</th>
<th>Admin/Oper</th>
</tr>
</thead>
<tbody>
<tr>
<td>node1</td>
<td>e0a</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0b</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0c</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0d</td>
<td>Default</td>
<td>-</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0e</td>
<td>Default</td>
<td>-</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0f</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0g</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td>node2</td>
<td>e0a</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
</tbody>
</table>
After you finish
You can use the unassigned ports to create the new broadcast domain.

Related references
*Information to gather before creating the IPspace, broadcast domain, and subnet configuration* on page 39

**Creating a broadcast domain for the IPspace (cluster administrators only)**

You must create a broadcast domain for the IPspace. A broadcast domain defines what network ports are grouped into the same Layer 2 network. The ports in a network domain can be used by the Storage Virtual Machines (SVMs) assigned to that IPspace.

**Before you begin**

- The IPspace to which you want to assign the broadcast domain must exist.
- You must already know which ports are unassigned and can be added to the new broadcast domain.

**About this task**

When you create a broadcast domain, a failover group for the broadcast domain is automatically created. The failover group contains all the ports assigned to the broadcast domain.

**Steps**

1. Create the broadcast domain by using the `network port broadcast-domain create` command.

   **Example**
   ```
   network port broadcast-domain create -ipspace ipspace1 -broadcast-domain -ipspace1 -mtu 1500 -ports node1:e0d,node1:e0e,node2:e0d,node2:e0e
   ```

2. Verify that the broadcast domain configuration is correct by using the following commands:

   a. `network port broadcast-domain show`
   b. `network port show`
   c. `network interface failover-groups show`

   **Example**
   ```
   network port broadcast-domain show
   ```

<table>
<thead>
<tr>
<th>IPspace</th>
<th>Broadcast Domain Name</th>
<th>MTU</th>
<th>Port List</th>
<th>Update Status</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster</td>
<td>Cluster</td>
<td>1500</td>
<td>node1:e0a,node1:e0b,node2:e0a</td>
<td>complete</td>
<td></td>
</tr>
</tbody>
</table>
network port show

<table>
<thead>
<tr>
<th>Node</th>
<th>Port</th>
<th>IPspace</th>
<th>Broadcast Domain</th>
<th>Link</th>
<th>MTU</th>
<th>Admin/Oper</th>
</tr>
</thead>
<tbody>
<tr>
<td>node1</td>
<td>e0a</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td>node1</td>
<td>e0b</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td>node1</td>
<td>e0c</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td>node1</td>
<td>e0d</td>
<td>ipspace1</td>
<td>ipspace1</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td>node1</td>
<td>e0e</td>
<td>ipspace1</td>
<td>ipspace1</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td>node1</td>
<td>e0f</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td>node1</td>
<td>e0g</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td>node2</td>
<td>e0a</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td>node2</td>
<td>e0b</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td>node2</td>
<td>e0c</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td>node2</td>
<td>e0d</td>
<td>ipspace1</td>
<td>ipspace1</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td>node2</td>
<td>e0e</td>
<td>ipspace1</td>
<td>ipspace1</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td>node2</td>
<td>e0f</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td>node2</td>
<td>e0g</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
</tbody>
</table>

network interface failover-groups show

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Group</th>
<th>Failover Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster</td>
<td>Cluster</td>
<td>node1:e0a, node1:e0b, node2:e0a, node2:e0b</td>
</tr>
<tr>
<td>cluster1</td>
<td>Default</td>
<td>node1:e0c, node1:e0f, node1:e0g, node2:e0c, node2:e0f, node2:e0g</td>
</tr>
<tr>
<td>ipspace1</td>
<td>ipspace1</td>
<td>node1:e0d, node1:e0e, node2:e0d, node2:e0e</td>
</tr>
</tbody>
</table>

After you finish

Next, you can create a subnet for the broadcast domain.

Related references

*Information to gather before creating the IPspace, broadcast domain, and subnet configuration* on page 39

Creating a subnet for the IPspace (cluster administrators only)

After you create the broadcast domain, you should create a subnet to allocate specific blocks of IPv4 or IPv6 addresses to be used later when you create LIFs for the Storage Virtual Machine (SVM). This
enables you to create LIFs more easily by specifying a subnet name instead of having to specify IP address and network mask values for each LIF.

**Before you begin**

The broadcast domain and IPspace to which you plan to add the subnet must already exist.

**About this task**

Although optional, you should use subnets when creating LIFs, because the use of subnets enables easier LIF management. The following subnet requirements apply:

- All subnet names must be unique within an IPspace.
- When adding IP address ranges to a subnet, you must ensure that there are no overlapping IP addresses in the routable network so that different subnets, or hosts, do not attempt to use the same IP address.
- The subnet must be routable to all external servers required for services such as Active Directory (AD) domain controllers, DNS, NIS, LDAP, and NDMP.

This CIFS server setup uses a subnet for assigning IP addresses, the netmask, and the default gateway to data LIFs. An alternative method is to create LIFs by providing the IP address and netmask and then creating the default gateway as a separate task. For more information about alternatives for configuring network solutions, see the *Clustered Data ONTAP Network Management Guide*.

**Steps**

1. Create the subnet by using the `network subnet create` command.

   **Example**

   ```
   network subnet create -broadcast-domain ipspace1 -ipspace ipspace1 -subnet-name ipspace1 -subnet 10.0.0.0/24 -gateway 10.0.0.1 -ip-ranges "10.0.0.128-10.0.0.130,10.0.0.132"
   ``

   The subnet name can be either a subnet IP value such as “192.0.2.0/24” or a string such as “ipspace1” like the one used in this example.

2. Verify that the subnet configuration is correct by using the `network subnet show` command.

   **Example**

   ```
   network subnet show -ipspace ipspace1
   ``

   The output from this example shows information about the subnet named “ipspace1” in the “ipspace1” IPspace. The subnet belongs to the broadcast domain name “ipspace1”. You can assign the IP addresses in this subnet to data LIFs for SVMs created in the “ipspace1” IPspace.

   ```
   IPspace: ipspace1
   Subnet Name    Subnet    Broadcast Domain    Gateway    Avail/Total    Ranges
   ----------------- ------------- -------------- ---------- -------------- ---------------
   ipspace1 10.0.0.0/24 ipspace1 10.0.0.1    4/4    10.0.0.128-10.0.0.130, 10.0.0.132
   ```

**After you finish**

- You must create a SVM to contain the CIFS server.
- You must then create the LIFs on the SVM, associating the subnet you just created to the LIFs.
Creating an SVM with FlexVol volumes for the CIFS server (cluster administrators only)

Prior to creating a CIFS server, you must create a Storage Virtual Machine (SVM) with a configuration that is appropriate for hosting the CIFS server.

**Before you begin**

The following prerequisites must be met before you create the SVM:

- The aggregate on which you want to create the SVM root volume must exist.
- If you want to create the SVM in an IPspace other than the default one, the IPspace must already exist.
- You must know which security style the root volume will have.

If you plan to implement a Hyper-V or SQL Server over SMB solution on this SVM, you should use NTFS security style for the root volume. Volumes that contain Hyper-V files or SQL database files must be set to NTFS security at the time they are created. By setting the root volume security style to NTFS, you ensure that you do not inadvertently create UNIX or mixed security-style data volumes.

**About this task**

For information about creating an SVM with Infinite Volume, see the *Clustered Data ONTAP Infinite Volumes Management Guide*.

For information about creating other types of SVMs, such as Data Protection or MetroCluster SVMs, see the *Clustered Data ONTAP Data Protection Guide* and the *MetroCluster Installation and Configuration Guide*.

**Steps**

1. Determine which aggregates are candidates for containing the SVM root volume by displaying information about all the aggregates in the cluster except for the ones that are node root aggregates:

   ```bash
   storage aggregate show --has-mroot false
   ```

   **Example**

   ```bash
   storage aggregate show --has-mroot false
   ```

<table>
<thead>
<tr>
<th>Aggregate</th>
<th>Size (GB)</th>
<th>Available (GB)</th>
<th>Used (%)</th>
<th>State</th>
<th>#Vols</th>
<th>Nodes</th>
<th>RAID Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>aggr1</td>
<td>239.0</td>
<td>229.8</td>
<td>4%</td>
<td>online</td>
<td>4</td>
<td>node1</td>
<td>raid_dp, normal</td>
</tr>
<tr>
<td>aggr2</td>
<td>239.0</td>
<td>235.9</td>
<td>1%</td>
<td>online</td>
<td>2</td>
<td>node2</td>
<td>raid_dp, normal</td>
</tr>
<tr>
<td>aggr3</td>
<td>478.1</td>
<td>465.2</td>
<td>3%</td>
<td>online</td>
<td>1</td>
<td>node2</td>
<td>raid_dp, normal</td>
</tr>
</tbody>
</table>

   The best practice is to use a separate aggregate for SVM root volumes. You should not create a root volume on an aggregate that contains data volumes.

   You must choose an aggregate that has at least 1 GB of free space to contain the root volume. If you intend to configure NAS auditing on the SVM, you must have a minimum of 3 GB of extra
free space on the root aggregate, with the extra space being used to create the auditing staging volume when auditing is enabled.

**Note:** If NAS auditing is already enabled on an existing SVM, the aggregate's staging volume is created immediately after aggregate creation is successfully completed.

2. Record the name of the aggregate on which you want to create the SVM root volume.

3. If you plan on specifying a language when you create the SVM and do not know the value to use, identify and record the value of the language you want to specify:
   
   ```
   vserver create -language ?
   ```

4. If you plan on specifying a Snapshot policy when you create the SVM and do not know the name of the policy, list the available policies and identify and record the name of the quota policy you want to use:
   
   ```
   volume snapshot policy show -vserver vserver_name
   ```

5. If you plan on specifying a quota policy when you create the SVM and do not know the name of the policy, list the available policies and identify and record the name of the quota policy you want to use:
   
   ```
   volume quota policy show -vserver vserver_name
   ```

6. Create the SVM:
   
   ```
   vserver create -vserver vserver_name -aggregate aggregate_name -rootvolume root_volume_name -rootvolume-security-style {unix|ntfs|mixed} [-ipspace IPspace_name] [-language language] [-snapshot-policy snapshot_policy_name] [-quota-policy quota_policy_name] [-comment comment]
   ```

   **Example**
   
   ```
   vserver create -vserver vsl -aggregate aggr3 -rootvolume vsl_root -rootvolume-security-style ntfs -ipspace ipspace1 -language en_US.UTF-8
   ```

   ![Job succeeded: Vserver creation completed]

7. Verify that the SVM configuration is correct by using the `vserver show` command.

   **Example**
   
   ```
   vserver show -vserver vsl
   ```

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment: default</td>
<td>Comment: default</td>
<td>Comment: default</td>
<td></td>
</tr>
<tr>
<td>List of Aggregates Assigned: -</td>
<td>List of Aggregates Assigned: -</td>
<td>List of Aggregates Assigned: -</td>
<td></td>
</tr>
<tr>
<td>Limit on Maximum Number of Volumes allowed: unlimited</td>
<td>Vserver Admin State: running</td>
<td>Vserver Admin State: running</td>
<td></td>
</tr>
<tr>
<td>Vserver Operational State: running</td>
<td>Vserver Operational State: running</td>
<td>Vserver Operational State: running</td>
<td></td>
</tr>
<tr>
<td>Allowed Protocols: nfs, cifs, ndmp</td>
<td>Disallowed Protocols: fcp, iscsi</td>
<td>Disallowed Protocols: fcp, iscsi</td>
<td></td>
</tr>
<tr>
<td>Is Vserver with Infinite Volume: false</td>
<td>Is Vserver with Infinite Volume: false</td>
<td>Is Vserver with Infinite Volume: false</td>
<td></td>
</tr>
</tbody>
</table>
In this example, the command creates the SVM named “vs1” in IPspace “ipspace1”. The root volume is named “vs1_root” and is created on aggr3 with NTFS security style.

**Related tasks**

*Modifying protocols for SVMs* on page 136

**Related references**

*Information to gather before configuring the SVM* on page 42

**Related information**

*Clustered Data ONTAP 8.3 Infinite Volumes Management Guide*
*Clustered Data ONTAP 8.3 Data Protection Guide*
*Clustered Data ONTAP 8.3 MetroCluster Installation and Configuration Guide*

**Creating LIFs on the SVM (cluster administrators only)**

Before you can provide SMB access to the CIFS server, you must create LIFs on the Storage Virtual Machine (SVM). The LIFs that you create must be routable to all external servers required for services such as Active Directory (AD) domain controllers, DNS, NIS, LDAP, and NDMP.

**Before you begin**

You must have the subnet name that you want to assign to the LIFs.

**About this task**

- You should not configure LIFs that carry CIFS traffic to automatically revert to their home nodes. This recommendation is mandatory if the CIFS server is to host a solution for nondisruptive operations with Hyper-V or SQL Server over SMB.
- There are several optional parameters that you might want to use to customize the LIF configuration.
  For more information about using optional parameters, see the *Clustered Data ONTAP Network Management Guide*.

**Steps**

1. Determine which of the IPspace broadcast domain ports you want to use for the LIFs by using the `network port broadcast-domain show` command.

**Example**

```bash
network port broadcast-domain show -ipspace ipspace1
```

<table>
<thead>
<tr>
<th>IPspace Name</th>
<th>Broadcast Domain Name</th>
<th>MTU Port List</th>
<th>Update Status Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipspace1</td>
<td>ipspace1</td>
<td>1500</td>
<td>node1:e0d complete</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>node1:e0e complete</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>node2:e0d complete</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>node2:e0e complete</td>
</tr>
</tbody>
</table>
2. Verify that the subnet that you want to use for the LIFs contains sufficient unused IP addresses by using the `network subnet show` command.

   **Example**
   
   ```
   network subnet show -ipspace ipspace1
   ```

<table>
<thead>
<tr>
<th>IPspace: ipspace1</th>
<th>Subnet</th>
<th>Broadcast</th>
<th>Gateway</th>
<th>Avail/Ranges</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipspace1</td>
<td>10.0.0.0/24</td>
<td>ipspace1</td>
<td>10.0.0.1</td>
<td>4/4 10.0.0.128-10.0.0.130, 10.0.0.132</td>
</tr>
</tbody>
</table>

3. Create one or more LIF interfaces on the ports that you want to use to access data over SMB on the SVM by using the `network interface create` command.

   **Example**
   
   ```
   network interface create -vserver vs1 -lif lif1 -role data -data-protocol nfs,cifs -home-node node1 -home-port e0d -subnet-name ipspace1
   network interface create -vserver vs1 -lif lif2 -role data -data-protocol nfs,cifs -home-node node2 -home-port e0d -subnet-name ipspace1
   ```

4. Verify that the LIF interface configuration is correct by using the `network interface show` command.

   **Example**
   
   ```
   network interface show -vserver vs1
   ```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Interface</th>
<th>Status</th>
<th>Network Address/Mask</th>
<th>Current Node</th>
<th>Current Port</th>
<th>Home</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>lif1</td>
<td>up/up</td>
<td>10.0.0.128/24</td>
<td>node1</td>
<td>e0d</td>
<td>true</td>
</tr>
<tr>
<td></td>
<td>lif2</td>
<td>up/up</td>
<td>10.0.0.129/24</td>
<td>node2</td>
<td>e0d</td>
<td>true</td>
</tr>
</tbody>
</table>

5. Verify that the failover group configuration is as desired by using the `network interface show` command with the `-failover` parameter.

   **Example**
   
   ```
   network interface show -failover -vserver vs1
   ```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Logical Interface</th>
<th>Home Node:Port</th>
<th>Failover Policy</th>
<th>Failover Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>lif1</td>
<td>node1:e0d</td>
<td>system-defined</td>
<td>ipspace1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failover Targets: node1:e0d, node1:e0e, node2:e0d, node2:e0e</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>lif2</td>
<td>node2:e0d</td>
<td>system-defined</td>
<td>ipspace1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failover Targets: node2:e0d, node2:e0e, node1:e0d, node1:e0e</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

After you finish

You must configure DNS name services for the SVM, after which you can create the CIFS server.
Configuring DNS services for the SVM

You must configure DNS services for the Storage Virtual Machine (SVM) before creating the CIFS server. Generally, the DNS name servers are the Active Directory-integrated DNS servers for the domain that the CIFS server will join.

About this task

Active Directory-integrated DNS servers contain the service location records (SRV) for the domain LDAP and domain controller servers. If the Storage Virtual Machine (SVM) cannot find the Active Directory LDAP servers and domain controllers, CIFS server setup fails.

Storage Virtual Machines (SVMs) use the **hosts** name services ns-switch database to determine which name services to use and in which order to use the them when looking up information about hosts. The two supported name services for the hosts database are **files** and **dns**.

You must ensure that **dns** is one of the sources before you create the CIFS server.

Steps

1. Determine what the current configuration is for the **hosts** name services database by using the `vserver services name-service ns-switch show` command.

   **Example**
   
   In this example, the **hosts** name service database uses the default settings.

   ```
   vserver services name-service ns-switch show -vserver vs1 -database hosts
   ```

<table>
<thead>
<tr>
<th>Vserver: vs1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name Service Switch Database: hosts</td>
</tr>
<tr>
<td>Name Service Source Order: files, dns</td>
</tr>
</tbody>
</table>

2. If needed, perform the following actions:

   a. Add the DNS name service to the **hosts** name service database in the desired order or reorder the sources by using the `vserver services name-service ns-switch modify` command.

      **Example**
      
      In this example, the **hosts** database is configured to use DNS and local files in that order.

      ```
      vserver services name-service ns-switch modify -vserver vs1 -database hosts -sources dns,files
      ```

   b. Verify that the name services configuration is correct by using the `vserver services name-service ns-switch show` command.

      **Example**
      
      ```
      vserver services name-service ns-switch show -vserver vs1 -database hosts
      ```
3. Configure DNS services by using the vserver services name-service dns create command.

Example

vserver services name-service dns create -vserver vs1 -domains example.com,example2.com -name-servers 10.0.0.50,10.0.0.51

4. Verify that the DNS configuration is correct and that the service is enabled by using the vserver services name-service dns show command.

Example

vserver services name-service dns show -vserver vs1

Vserver: vs1
Name Service Switch Database: hosts
Name Service Source Order: dns, files

<table>
<thead>
<tr>
<th>Vserver: vs1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name Service: example.com, example2.com</td>
</tr>
<tr>
<td>Name Servers: 10.0.0.50, 10.0.0.51</td>
</tr>
<tr>
<td>Enable/Disable DNS: enabled</td>
</tr>
<tr>
<td>Timeout (secs): 2</td>
</tr>
<tr>
<td>Maximum Attempts: 1</td>
</tr>
</tbody>
</table>

Related references

Information to gather before configuring name services on page 45

Configuring dynamic DNS on the SVM

If you want the Active Directory-integrated DNS server to dynamically register the CIFS server’s DNS records in DNS, you must configure dynamic DNS (DDNS) on the Storage Virtual Machine (SVM) before creating the CIFS server.

Before you begin

DNS name services must be configured on the SVM. If you are using secure DDNS, you must use Active-Directory integrated DNS name servers.

Steps

1. Configure DDNS on the SVM:

   vserver services name-service dns dynamic-update modify -vserver vserver_name -is-enabled true [-use-secure {true|false} -domain-name FQDN_used_for_DNS_updates

   Example

   vserver services name-service dns dynamic-update modify -vserver vs1 -is-enabled true -use-secure true -domain-name example.com

2. Verify that the DDNS configuration is correct:

   vserver services name-service dns dynamic-update show

   Example

   vserver services name-service dns dynamic-update show
Creating a CIFS server

A CIFS server is necessary to provide SMB clients with access to the Storage Virtual Machine (SVM). After you set up DNS services on the SVM, you can create a CIFS server.

Before you begin

- At least one SVM LIF must exist on the SVM.
- The LIFs must be able to connect to the DNS servers configured on the SVM and to an Active Directory domain controller of the domain to which you want to join the CIFS server.
- The DNS servers must contain the service location records that are needed to locate the Active Directory domain services.
- The cluster time must be synchronized to within five minutes of the Active Directory domain controller's time.
  You should configure cluster NTP services to use the same NTP servers for time synchronization as the Active Directory domain uses.

About this task

You must keep the following in mind when creating the CIFS server:

- The CIFS server name might or might not be the same as the SVM name.
- The CIFS server name can be up to 15 characters in length.
  The following characters are not allowed: @ # * ( ) = + [ ] | ; : " , < > \ / ?
- You must use the FQDN when specifying the domain.
- The default is to add the CIFS server machine account to the Active Directory CN=Computer object.
- You can choose to add the CIFS server to a different organizational unit (OU) by using the -ou option.
  When specifying the OU, you do not specify the domain portion of the distinguished name, you only specify the OU or CN portion of the distinguished name. Data ONTAP appends the value provided for the required -domain parameter onto the value provided for the -ou parameter to produce the Active Directory distinguished name, which is used when joining the Active Directory domain.
- You can optionally choose to add a text comment of up to 256 characters about the CIFS server. If there is a space in the comment text, you must enclose the entire string in quotation marks.
- You can optionally choose to add a comma-delimited list of one or more NetBIOS aliases (up to 200) for the CIFS server.
  A NetBIOS alias name can be up to 15 characters in length. The following characters are not allowed: @ # * ( ) = + [ ] | ; : " , < > \ / ?
- The initial administrative status of the CIFS server is up.

Steps

1. Create the CIFS server on the SVM:
vserver cifs create -vserver vserver_name -domain FQDN [-ou organizational_unit] [-comment text] [-netbios-aliases NetBIOS_name, ...]

When joining a domain, this command might take several minutes to complete.

Example

vserver cifs create -vserver vs1 -name CIFS1 -domain example.com

2. Verify the CIFS server configuration by using the vserver cifs show command.

Example

In this example, the command output shows that a CIFS server named “CIFS1” was created on SVM vs1 and was joined to the example.com domain.

vserver cifs show -vserver vs1

| Vserver: vs1 |
| CIFS Server NetBIOS Name: CIFS1 |
| NetBIOS Domain/Workgroup Name: EXAMPLE |
| Fully Qualified Domain Name: EXAMPLE.COM |
| Default Site Used by LIFs Without Site Membership: |
| Authentication Style: domain |
| CIFS Server Administrative Status: up |
| CIFS Server Description: - |
| List of NetBIOS Aliases: - |

Examples

The following command creates a CIFS server named “CIFS2” on SVM vs1 in the example.com domain. The machine account is created in the OU=eng,OU=corp,DC=example,DC=com container. The CIFS server is assigned an NetBIOS alias.

cluster1::> vserver cifs create -vserver vs1 -cifs-server CIFS2 -domain example.com -ou OU=eng,OU=corp -netbios-aliases CIFS4

cluster1::> vserver cifs show -vserver vs1

Vserver: vs1
CIFS Server NetBIOS Name: CIFS2
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership: |
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description: -
List of NetBIOS Aliases: CIFS4

The following command enables the administrator of a trusted domain to create a CIFS server named “CIFS3” on SVM vs1. The -domain option specifies the name of the home domain (specified in the DNS configuration) in which you want to create the CIFS server. The username option specifies the administrator of the trusted domain.

Home domain: example.com
Trusted domain: trust.lab.com
Username for the trusted domain: Administrator1

cluster1::> vserver cifs create -vserver vs1 -cifs-server CIFS3 -domain example.com

Username: Administrator1@trust.lab.com
Password: . . .
About this task

Storage Virtual Machines (SVMs) use the name services ns-switch databases to determine the order in which to look up the sources for a given name service database. If you are using LDAP or NIS name services, you must customize the name services database configuration to match your name service infrastructure before configuring LDAP or NIS name services.

The default is to have the CIFS server map all Windows users to the default UNIX user that is stored in the local passwd database. If you want to use the default configuration, configuring NIS or LDAP UNIX user and group name services or LDAP user mapping is optional for SMB access.

Steps

1. Optional: If UNIX users, group, and netgroup information is managed by NIS name services, configure NIS name services:
   a. Determine the current ordering of name services by using the vserver services name-service ns-switch show command.

   Example

   In this example, the three database that can use nis as a name service source (the group, passwd, and netgroup databases) are using only files as a source.

   vserver services name-service ns-switch show -vserver vs1
You must add the **nis** source to the **group** and **passwd** databases, and optionally to the **netgroup** database.

b. Adjust the name service ns-switch database ordering as desired by using the `vserver services name-service ns-switch modify` command.

For best performance, you should not add a name-service to a name service database unless you plan on configuring that name service on the SVM.

If you modify the configuration for more than one name service database, you must run the command separately for each name service database that you want to modify.

**Example**

In this example, **nis** and **files** are configured as sources for the **group** and **passwd** databases, in that order. The rest of the name service databases are unchanged.

```
vserver services name-service ns-switch modify -vserver vs1 -database group -sources nis,files
vserver services name-service ns-switch modify -vserver vs1 -database passwd -sources nis,files
```

c. Verify that the ordering of name services is correct by using the `vserver services name-service ns-switch show` command.

**Example**

```
vserver services name-service ns-switch show -vserver vs1
```

d. Create the NIS name service configuration:

```
vserver services name-service nis-domain create -vserver vserver_name -domain NIS_domain_name -servers NIS_server_IPaddress,... -active true
```

**Example**

```
vserver services name-service nis-domain create -vserver vs1 -domain example.com -servers 10.0.0.60 -active true
```

e. Verify that the NIS name service is properly configured and active:

```
vserver services name-service nis-domain show vserver vserver_name
```
Example

```
vserver services name-service nis-domain show vserver vs1
```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Domain</th>
<th>Active</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>example.com</td>
<td>true</td>
<td>10.0.0.60</td>
</tr>
</tbody>
</table>

2. Optional: If UNIX users, group, and netgroup information or name mapping is managed by LDAP name services, configure LDAP name services by using the information located in the *Clustered Data ONTAP File Access Management Guide for NFS*.

Related references

- *Information to gather before configuring name services* on page 45

Related information

- *Clustered Data ONTAP 8.3 File Access Management Guide for NFS*

Where to find information about SMB support on Infinite Volumes

For information about the SMB versions and functionality that Infinite Volumes support, see the *Clustered Data ONTAP Infinite Volumes Management Guide*.

Related information

- *Clustered Data ONTAP 8.3 Infinite Volumes Management Guide*
Managing CIFS servers

After you set up a CIFS server, you can perform management tasks. For example, you can configure CIFS server options, manage CIFS server security settings, configure SMB and SMB signing, configure LDAP over SSL/TLS, manage oplocks, configure IPv6 SMB access, apply GPOs to CIFS servers, manage domain controller connections, and manage the CIFS server service.

Related concepts

Using options to customize CIFS servers on page 70
Managing CIFS server security settings on page 79
Configuring SMB on your CIFS server on page 103
Using SMB signing to enhance network security on page 85
Using LDAP over SSL/TLS to secure communication on page 95
Improving client performance with traditional and lease oplocks on page 107
Using IPv6 for SMB access and CIFS services on page 141
Applying Group Policy Objects to CIFS servers on page 113
Managing domain controller connections on page 130
Changing CIFS servers computer account passwords on page 128
Managing NetBIOS aliases for CIFS servers on page 132
Managing miscellaneous CIFS server tasks on page 135
Using local users and groups for authentication and authorization on page 212
Managing file locks on page 294
Monitoring SMB activity on page 298
Managing how file security is presented to SMB clients for UNIX security-style data on page 75

Related tasks

Stopping or starting the CIFS server on page 136
Configuring access restrictions for anonymous users on page 74
Configuring character mapping for SMB file name translation on FlexVol volumes on page 161

Using options to customize CIFS servers

You can use options to customize CIFS servers, for example, to configure the default UNIX user. At the advanced privilege level, you can also enable or disable local Windows users and groups and local Windows user authentication, automatic node referrals and remote copy offload, export policies for SMB access, and other options.

Available CIFS server options

It is useful to know what options are available when considering how to customize the CIFS server. Although some options are for general use on the CIFS server, several are used to enable and configure specific CIFS functionality.

The following list specifies the CIFS server options available at admin privilege level:

• Configuring the SMB/CIFS session timeout value

Configuring this option enables you to specify the number of seconds of idle time before an SMB/CIFS session is disconnected. An idle session is a session in which a user does not have any files or directories opened on the client. The default value is 900 seconds.
• **Configuring the default UNIX group**
  Configuring this option enables you to specify the name of the default UNIX group for the CIFS server. There is no default value. This option is supported only on SVMs with Infinite Volume.

• **Configuring the default UNIX user**
  Configuring this option enables you to specify the default UNIX user that the CIFS server uses. Starting with Data ONTAP 8.2, Data ONTAP automatically creates a default user named “pcuser” (with a UID of 65534), creates a group named “pcuser” (with a GID of 65534), and adds the default user to the “pcuser” group. When you create a CIFS server, Data ONTAP automatically configures “pcuser” as the default UNIX user.

• **Configuring the guest UNIX user**
  Configuring this option enables you to specify the name of a UNIX user to which users who log in from untrusted domains are mapped, which allows a user from an untrusted domain to connect to the CIFS server. By default, this option is not configured (there is no default value); therefore, the default is to not allow users from untrusted domains to connect to the CIFS server.

• **Enabling or disabling read grants execute for mode bits**
  Enabling or disabling this option allows you to specify whether to allow SMB clients to run executable files with UNIX mode bits to which they have read access, even when the UNIX executable bit is not set. This option is disabled by default.

• **Enabling or disabling the ability to delete read-only files from NFS clients**
  Enabling or disabling this option determines whether to allow NFS clients to delete files or folders with the read-only attribute set. NTFS delete semantics do not allow deletion of a file or folder when the read-only attribute is set. UNIX delete semantics ignores the read-only bit, using the parent directory permissions instead to determine whether a file or folder can be deleted. The default setting is disabled, which results in NTFS delete semantics.

• **Configuring Windows Internet Name Service (WINS) server addresses**
  Configuring this option enables you to specify a list of WINS server addresses as a comma-delimited list. You must specify IPv4 addresses. IPv6 addresses are not supported. There is no default value.

The following list specifies the CIFS server options available at advanced privilege level:

• **Enabling or disabling SMB 2.x**
  SMB 2.0 is the minimum SMB version that supports LIF failover. If you disable SMB 2.x, Data ONTAP also automatically disables SMB 3.0. This option is supported only on SVMs with FlexVol volumes. The option is enabled by default on SVMs with FlexVol volumes, and disabled by default on SVMs with Infinite Volume.

• **Enabling or disabling SMB 3.0**
  SMB 3.0 is the minimum SMB version that supports continuously available shares. Windows Server 2012 and Windows 8 are the minimum Windows versions to support SMB 3.0. This option is supported only on SVMs with FlexVol volumes. The option is enabled by default on SVMs with FlexVol volumes, and disabled by default on SVMs with Infinite Volume.

• **Enabling or disabling ODX copy offload**
  ODX copy offload is used automatically by Windows clients that support it. This option is enabled by default.

• **Enabling or disabling the direct-copy mechanism for ODX copy offload**
  The direct-copy mechanism increases the performance of the copy offload operation when Windows clients try to open the source file of a copy in a mode that prevents the file being changed while the copy is in progress. By default, the direct copy mechanism is enabled.

• **Enabling or disabling automatic node referrals**
With automatic node referrals, the CIFS server automatically refers clients to a data LIF local to
the node that hosts the data accessed through the requested share. This option must be disabled on
Hyper-V over SMB configurations. This option is disabled by default.

- **Enabling or disabling export policies for SMB**
The default is to disable export policies for SMB.

- **Enabling or disabling using junction points as reparse points**
  If this option is enabled, the CIFS server exposes junction points to SMB clients as reparse points.
  This option is only valid for SMB 2.x or SMB 3.0 connections. This option is enabled by default.
  This option is supported only on SVMs with FlexVol volumes. The option is enabled by default
  on SVMs with FlexVol volumes, and disabled by default on SVMs with Infinite Volume.

- **Configuring the number of maximum simultaneous operations per TCP connection**
The default value is 255.

- **Enabling or disabling local Windows users and groups functionality**
  This option is enabled by default.

- **Enabling or disabling local Windows users authentication**
  This option is enabled by default.

- **Enabling or disabling VSS shadow copy functionality**
  Data ONTAP uses shadow copy functionality to perform remote backups of data stored using the
  Hyper-V over SMB solution.
  This option is supported only on SVMs with FlexVol volumes, and only for Hyper-V over SMB
  configurations. The option is enabled by default on SVMs with FlexVol volumes, and disabled by
  default on SVMs with Infinite Volume.

- **Configuring the shadow copy directory depth**
  Configuring this option enables you to define the maximum depth of directories on which to
  create shadow copies when using the shadow copy functionality.
  This option is supported only on SVMs with FlexVol volumes, and only for Hyper-V over SMB
  configurations. The option is enabled by default on SVMs with FlexVol volumes, and disabled by
  default on SVMs with Infinite Volume.

- **Enabling or disabling multidomain search capabilities for name mapping**
  If enabled, when a UNIX user is mapped to a Windows domain user by using a wildcard (*) in
  the domain portion of the Windows user name (for example, *joe), Data ONTAP searches for the
  specified user in all domains with bidirectional trusts to the home domain. The home domain is
  the domain that contains the CIFS server’s computer account.
  As an alternative to searching all bidirectionally trusted domains, you can configure a list of
  preferred trusted domains. If this option is enabled and a preferred list is configured, the preferred
  list is used to perform multidomain name mapping searches.
  The default is to enable multidomain name mapping searches.

- **Configuring the file system sector size**
  Configuring this option enables you to configure the file system sector size in bytes that Data
  ONTAP reports to SMB clients. There are two valid values for this option: **4096** and **512**. The
default value is **4096**. You might need to set this value to **512** if the Windows application
  supports only a sector size of 512 bytes.

- **Enabling or disabling Dynamic Access Control (DAC)**
  Enabling this option enables you to secure objects on the CIFS server by using Dynamic Access
  Control, including using auditing to stage central access policies and using Group Policy Objects
  to implementing central access policies. The option is disabled by default.
  This option is supported only on SVMs with FlexVol volumes.
• **Setting the access restrictions for non-authenticated sessions (restrict anonymous)**
  Setting this option determines what the access restrictions are for non-authenticated sessions. The restrictions are applied to the anonymous user. By default, there are no access restrictions for anonymous users.

• **Enabling or disabling the presentation of NTFS ACLs on volumes with UNIX effective security (UNIX security-style volumes or mixed security-style volumes with UNIX effective security)**
  Enabling or disabling this option determines how file security on files and folders with UNIX security is presented to SMB clients. If enabled, Data ONTAP presents files and folders in volumes with UNIX security to SMB clients as having NTFS file security with NTFS ACLs. If disabled, Data ONTAP presents volumes with UNIX security as FAT volumes, with no file security. By default, volumes are presented as having NTFS file security with NTFS ACLs.

• **Enabling or disabling the SMB fake open functionality**
  Enabling this functionality improves SMB 2.x and SMB 3.0 performance by optimizing how Data ONTAP makes open and close requests when querying for attribute information on files and directories. By default, SMB fake open functionality is enabled. This option is useful only for connections made with SMB 2.x or later.

• **Enabling or disabling the UNIX extensions**
  Enabling this option enables UNIX extensions on a CIFS server. UNIX extensions allow POSIX/UNIX style security to be displayed through the SMB protocol. By default this option is disabled. If you have UNIX-based SMB clients such as Mac OSX clients in your environment, you should enable UNIX extensions. Enabling UNIX extensions allows the CIFS server to transmit POSIX/UNIX security information over SMB to the UNIX-based client, which then translates the security information into POSIX/UNIX security.

• **Enabling or disabling support for short name searches**
  Enabling this option allows the CIFS server to perform searches on short names. A search query with this option enabled tries to match 8.3 file names along with long file names. The default value for this parameter is false.

• **Enabling or disabling support for automatic advertisement of DFS capabilities**
  Enabling or disabling this option determines whether CIFS servers automatically advertise DFS capabilities to SMB 2.x and SMB 3.0 clients that are connecting to shares. Clustered Data ONTAP uses DFS referrals in the implementation of symbolic links for SMB access. If enabled, the CIFS server always advertises DFS capabilities regardless of whether symbolic link access is enabled. If disabled, the CIFS server advertises DFS capabilities only when the clients are connecting to shares where symbolic link access is enabled.

**Related concepts**

- *Managing how file security is presented to SMB clients for UNIX security-style data* on page 75
- *Configuring SMB on your CIFS server* on page 103
- *Configuring multidomain name-mapping searches* on page 166
- *Securing file access by using Dynamic Access Control (DAC)* on page 196
- *Securing SMB access using export policies* on page 205
- *Using local users and groups for authentication and authorization* on page 212
- *Improving Microsoft remote copy performance* on page 359
- *Improving client response time by providing SMB automatic node referrals with Auto Location* on page 364
- *Configuring Data ONTAP for Microsoft Hyper-V and SQL Server over SMB solutions* on page 373
- *Share-based backups with Remote VSS* on page 378
- *Configuring SMB client access to UNIX symbolic links* on page 330
Related tasks

- Configuring CIFS server options on page 74
- Configuring access restrictions for anonymous users on page 74
- Enabling or disabling the presentation of NTFS ACLs for UNIX security-style data on page 76
- Configuring the default UNIX user on page 99

Related information

- Clustered Data ONTAP 8.3.1 man page: vserver cifs options modify - Modify CIFS options

Configuring CIFS server options

You can configure CIFS server options at any time after you have created a CIFS server on a Storage Virtual Machine (SVM)

Step

1. Perform the desired action:

<table>
<thead>
<tr>
<th>If you want to configure CIFS server options...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>At admin-privilege level</td>
<td>vserver cifs options modify -vserver vserver_name options</td>
</tr>
<tr>
<td>At advanced-privilege level</td>
<td>a. set -privilege advanced</td>
</tr>
<tr>
<td></td>
<td>b. vserver cifs options modify -vserver vserver_name options</td>
</tr>
<tr>
<td></td>
<td>c. set -privilege admin</td>
</tr>
</tbody>
</table>

Options is a list of one or more CIFS server options.

For more information about configuring CIFS server options, see the man page for the vserver cifs options modify command.

Related information

- Clustered Data ONTAP 8.3.1 man page: vserver cifs options modify - Modify CIFS options

Configuring access restrictions for anonymous users

By default, an anonymous, unauthenticated user (also known as the null user) can access certain information on the network. You can use a CIFS server option to configure access restrictions for the anonymous user.

About this task

The -restrict-anonymous CIFS server option corresponds to the RestrictAnonymous registry entry in Windows.

Anonymous users can list or enumerate certain types of system information from Windows hosts on the network, including user names and details, account policies, and share names. You can control access for the anonymous user by specifying one of three access restriction settings:
<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no-restriction</td>
<td>Specifies no access restrictions for anonymous users.</td>
</tr>
<tr>
<td>(default)</td>
<td></td>
</tr>
<tr>
<td>no-enumeration</td>
<td>Specifies that only enumeration is restricted for anonymous users.</td>
</tr>
<tr>
<td>no-access</td>
<td>Specifies that access is restricted for anonymous users.</td>
</tr>
</tbody>
</table>

**Steps**

1. Set the privilege level to advanced:
   ```
   set -privilege advanced
   ```

2. Configure the restrict anonymous setting:
   ```
   vserver cifs options modify -vserver vserver_name -restrict-anonymous
   {no-restriction|no-enumeration|no-access}
   ```

3. Verify that the option is set to the desired value:
   ```
   vserver cifs options show -vserver vserver_name
   ```

4. Return to the admin privilege level:
   ```
   set -privilege admin
   ```

**Related references**

Available CIFS server options on page 70

**Related information**

Clustered Data ONTAP 8.3.1 man page: vserver cifs options modify - Modify CIFS options

**Managing how file security is presented to SMB clients for UNIX security-style data**

You can choose how you want to present file security to SMB clients for UNIX security-style data by enabling or disabling the presentation of NTFS ACLs to SMB clients. There are advantages with each setting, which you should understand to choose the setting best suited for your business requirements.

By default, Data ONTAP presents UNIX permissions on UNIX security-style volumes to SMB clients as NTFS ACLs. There are scenarios where this is desirable, including the following:

- You want to view and edit UNIX permissions by using the Security tab in the Windows Properties box.
  You cannot modify permissions from a Windows client if the operation is not permitted by the UNIX system. For example, you cannot change the ownership of a file you do not own, because the UNIX system does not permit this operation. This restriction prevents SMB clients from bypassing UNIX permissions set on the files and folders.

- Users are editing and saving files on the UNIX security-style volume by using certain Windows applications, for example Microsoft Office, where Data ONTAP must preserve UNIX permissions during save operations.

- There are certain Windows applications in your environment that expect to read NTFS ACLs on files they use.
Under certain circumstances, you might want to disable the presentation of UNIX permissions as NTFS ACLs. If this functionality is disabled, Data ONTAP presents UNIX security-style volumes as FAT volumes to SMB clients. There are specific reasons why you might want to present UNIX security-style volumes as FAT volumes to SMB clients:

- You only change UNIX permissions by using mounts on UNIX clients. The Security tab is not available when a UNIX security-style volume is mapped on an SMB client. The mapped drive appears to be formatted with the FAT file system, which has no file permissions.
- You are using applications over SMB that set NTFS ACLs on accessed files and folders, which can fail if the data resides on UNIX security-style volumes. If Data ONTAP reports the volume as FAT, the application does not try to change an ACL.

Related concepts

*How security styles affect data access* on page 20

Related tasks

*Configuring security styles on FlexVol volumes* on page 147
*Configuring security styles on qtrees* on page 147

Related information

*Clustered Data ONTAP 8.3.1 man page: vserver cifs options modify - Modify CIFS options*

Enabling or disabling the presentation of NTFS ACLs for UNIX security-style data

You can enable or disable the presentation of NTFS ACLs to SMB clients for UNIX security-style data (UNIX security-style volumes and mixed security-style volumes with UNIX effective security).

About this task

If you enable this option, Data ONTAP presents files and folders on volumes with effective UNIX security style to SMB clients as having NTFS ACLs. If you disable this option, the volumes are presented as FAT volumes to SMB clients. The default is to present NTFS ACLs to SMB clients.

Steps

1. Set the privilege level to advanced:
   
   ```
   set -privilege advanced
   ```

2. Configure the UNIX NTFS ACL option setting:

   ```
   vserver cifs options modify -vserver vserver_name -is-unix-nt-acl-enabled {true|false}
   ```

3. Verify that the option is set to the desired value:

   ```
   vserver cifs options show -vserver vserver_name
   ```

4. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Related information

*Clustered Data ONTAP 8.3.1 man page: vserver cifs options modify - Modify CIFS options*
How Data ONTAP preserves UNIX permissions

When files in a FlexVol volume that currently have UNIX permissions are edited and saved by Windows applications, Data ONTAP can preserve the UNIX permissions.

When applications on Windows clients edit and save files, they read the security properties of the file, create a new temporary file, apply those properties to the temporary file, and then give the temporary file the original file name.

When Windows clients perform a query for the security properties, they receive a constructed ACL that exactly represents the UNIX permissions. The sole purpose of this constructed ACL is to preserve the file's UNIX permissions as files are updated by Windows applications to ensure that the resulting files have the same UNIX permissions. Data ONTAP does not set any NTFS ACLs using the constructed ACL.

How to manage UNIX permissions using the Windows Security tab

If you want to manipulate UNIX permissions of files or folders in mixed security-style volumes or qtrees on Storage Virtual Machines (SVMs) with FlexVol volumes, you can use the Security tab on Windows clients. Alternatively, you can use applications that can query and set Windows ACLs.

• Modifying UNIX permissions
  You can use the Windows Security tab to view and change UNIX permissions for a mixed security-style volume or qtree. If you use the main Windows Security tab to change UNIX permissions, you must first remove the existing ACE you want to edit (this sets the mode bits to 0) before you make your changes. Alternatively, you can use the Advanced editor to change permissions.
  If mode permissions are used, you can directly change the mode permissions for the listed UID, GID, and others (everyone else with an account on the computer). For example, if the displayed UID has r-x permissions, you can change the UID permissions to rwx.

• Changing UNIX permissions to NTFS permissions
  You can use the Windows Security tab to replace UNIX security objects with Windows security objects on a mixed security-style volume or qtree where the files and folders have a UNIX effective security style.
  You must first remove all listed UNIX permission entries before you can replace them with the desired Windows User and Group objects. You can then configure NTFS-based ACLs on the Windows User and Group objects. By removing all UNIX security objects and adding only Windows Users and Groups to a file or folder in a mixed security-style volume or qtree, you change the effective security style on the file or folder from UNIX to NTFS.
  When changing permissions on a folder, the default Windows behavior is to propagate these changes to all subfolders and files. Therefore, you must change the propagation choice to the desired setting if you do not want to propagate a change in security style to all child folders, subfolders, and files.

How to control automatic DFS advertisements in clustered Data ONTAP with a CIFS server option

A CIFS server option has been added that controls how DFS capabilities are advertised to SMB clients when connecting to shares. Because clustered Data ONTAP uses DFS referrals when clients access symbolic links over SMB, you should be aware of what the impact is when disabling or enabling this option.

In clustered Data ONTAP 8.2 through 8.2.2, the CIFS servers on Storage Virtual Machines (SVMs) always advertise to SMB clients that they are DFS capable. However, even though the CIFS servers always advertise that they are DFS capable, symbolic link access for SMB is managed on a share-by-share basis by setting a share parameter. By using the share parameter, you can set symbolic link access for SMB to one of three access levels:
• Enabled for read and write access
• Enabled for read-only access
• Disabled, either by setting the value of this parameter to hide symlinks or by setting the parameter to null (""")

Starting with Data ONTAP 8.2.3 in the 8.2 release family and with Data ONTAP 8.3 and later, a CIFS server option determines whether the CIFS servers automatically advertise that they are DFS capable to SMB clients. By default, this option is enabled and the CIFS server always advertises that it is DFS capable to SMB clients (even when connecting to shares where access to symbolic links is disabled). If you want the CIFS server to advertise that it is DFS capable to clients only when they are connecting to shares where access to symbolic links is enabled, you can disable this option.

You should be aware of what happens when this option is disabled:

• The share configurations for symbolic links is unchanged.
• If the share parameter is set to allow symbolic link access (either read-write access or read-only access), the CIFS server advertises DFS capabilities to clients connecting to that share. Client connections and access to symbolic links continue without interruption.
• If the share parameter is set to not allow symbolic link access (either by disabling access or if the value for the share parameter is null), the CIFS server does not advertise DFS capabilities to clients connecting to that share. Because clients have cached information that the CIFS server is DFS capable and it is no longer advertising that it is, clients that are connected to shares where symbolic link access is disabled might not be able to access these shares after the CIFS server option is disabled. After the option is disabled, you might need to reboot clients that are connected to these shares, thus clearing the cached information.

These changes do not apply to SMB 1.0 connections.

**Managing whether the CIFS server automatically advertises DFS capabilities**

You can set a CIFS server option to determine whether CIFS servers automatically advertise DFS capabilities to SMB 2.x and SMB 3.0 clients connecting to shares. You can disable automatic advertisements in cases where you have applications that will not make connections to shares that advertise DFS capabilities.

**About this task**

Clustered Data ONTAP uses DFS referrals in the implementation of symbolic links for SMB access. You should keep the following in mind when deciding whether to enable or disable this option:

• If automatic DFS advertisements are enabled, the CIFS server always advertises DFS capabilities to SMB 2.x and SMB 3.0 clients connecting to a share regardless of whether symbolic link access for CIFS is enabled on that share. This is the default setting.
• If automatic DFS advertisements are disabled, the CIFS server advertises DFS capabilities to SMB 2.x and SMB 3.0 clients only when the clients are connecting to shares where symbolic link access is enabled (either read-write or read-only access) and does not advertise DFS capabilities to clients if they are connecting to shares where symbolic link access is disabled.

Clients that are connected to shares where symbolic link access is disabled might not be able to access these shares after the CIFS server option is disabled. This is because the clients have cached information that the CIFS server is DFS capable, and it is no longer advertising that it is. This causes reconnections to SMB shares to fail. There are two ways to manage this:
• Before disabling the option, you can change the share setting on all shares to allow either read-write or read-only access.

• If it is not possible to change the settings for shares where symbolic link access is disabled, after the option is disabled, you can reboot any affected clients that are connected to these shares, thus clearing the cached information.

Steps
1. Set the privilege level to advanced:
   `set -privilege advanced`
2. Configure the DFS referral option setting:
   `vserver cifs options modify -vserver vserver_name -is-advertise-dfs-enabled {true|false}`
3. Verify that the option is set to the desired value:
   `vserver cifs options show -vserver vserver_name`
4. Return to the admin privilege level:
   `set -privilege admin`

Managing CIFS server security settings

You can customize CIFS server security settings to meet your business requirements. You can modify Kerberos security settings, determine whether to require SMB signing for incoming SMB traffic, whether to use LDAP over SSL/TLS, whether to enable AES encryption types for Kerberos communication, whether to require SMB encryption when accessing shares, and whether to require password complexity for local users. You can also set the minimum authentication security level.

Important considerations about CIFS server security settings in an SVM disaster recovery configuration

Before creating a Storage Virtual Machine (SVM) that is configured as a disaster recovery destination where the identity is not preserved (the `-identity-preserve` option is set to `false` in the SnapMirror configuration), there is important considerations that you should know about how CIFS server security settings are managed on the destination SVM.

The non-default CIFS server security settings are not replicated to the destination. When you create a CIFS server on the destination SVM, all CIFS server security settings are set to default values. When the SVM disaster recovery destination is initialized, updated, or resynced, the CIFS server security settings on the source are not replicated to the destination.

If you have non-default CIFS server security settings configured on the source SVM, you must manually configure these same settings on the destination SVM after the destination becomes read-write (after the SnapMirror relationship is broken).

Displaying information about CIFS server security settings

You can display information about CIFS server security settings on your Storage Virtual Machines (SVMs). You can use this information to verify that the security settings are correct.

About this task

A displayed security setting can be the default value for that object or a non-default value configured either by using the Data ONTAP CLI or by using Active Directory group policy objects (GPOs).
Step

1. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want display information about...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>All security settings on a specified SVM</td>
<td><code>vserver cifs security show -vserver vserver_name</code></td>
</tr>
<tr>
<td>A specific security setting or settings on the SVM</td>
<td><code>vserver cifs security show -vserver vserver_name -fields [fieldname,...]</code></td>
</tr>
<tr>
<td>You can enter <code>-fields ?</code> to determine what fields you can use.</td>
<td></td>
</tr>
</tbody>
</table>

Examples

The following example shows all security settings for SVM vs1:

```
cluster1::> vserver cifs security show -vserver vs1
Vserver: vs1
    Kerberos Clock Skew:                   5 minutes
    Kerberos Ticket Age:                  10 hours
    Kerberos Renewal Age:                   7 days
    Kerberos KDC Timeout:                   3 seconds
    Is Signing Required:               false
    Is Password Complexity Required:                true
    Use start_tls For AD LDAP connection:               false
    Is AES Encryption Enabled:               false
    LM Compatibility Level:  lm-ntlm-ntlmv2-krb
    Is SMB Encryption Required:               false
```

The following example shows the Kerberos clock skew for SVM vs1:

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-clock-skew

vserver kerberos-clock-skew
------- -------------------
vs1     5
```

Related tasks

* Displaying information about GPO configurations on page 120

Enabling or disabling required password complexity for local SMB users

Required password complexity provides enhanced security for local SMB users on your Storage Virtual Machines (SVMs) and is enabled by default. You can disable it and reenable it at any time.

Before you begin

Local users and groups and local user authentication must be enabled on the CIFS server.

Steps

1. Perform one of the following actions:
If you want required password complexity for local SMB users to be...

<table>
<thead>
<tr>
<th>Enabled</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>vserver cifs security modify -vserver vserver_name -is-password-complexity-required true</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Disabled</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>vserver cifs security modify -vserver vserver_name -is-password-complexity-required false</td>
<td></td>
</tr>
</tbody>
</table>

2. Verify the security setting for required password complexity:

```
 vserver cifs security show -vserver vserver_name
```

Example

The following example shows that required password complexity is enabled for local SMB users for SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password-complexity-required true
cluster1::> vserver cifs security show -vserver vs1 -fields is-password-complexity-required
vserver is-password-complexity-required
------- -------------------------------
vs1     true
```

Related concepts

- Using local users and groups for authentication and authorization on page 212
- Requirements for local user passwords on page 217

Related tasks

- Displaying information about CIFS server security settings on page 79
- Changing local user account passwords on page 224

Modifying the CIFS server Kerberos security settings

You can modify certain CIFS server Kerberos security settings, including the maximum allowed Kerberos clock slew time, the Kerberos ticket lifetime, and the maximum number of ticket renewal days.

About this task

Modifying CIFS server Kerberos settings by using the `vserver cifs security modify` command modifies the settings only on the single Storage Virtual Machine (SVM) that you specify with the `-vserver` parameter. You can centrally manage Kerberos security settings for all SVMs on the cluster belonging to the same Active Directory domain by using Active Directory group policy objects (GPOs).

Steps

1. Perform one or more of the following actions:
If you want to... Enter...

Specify the maximum allowed Kerberos clock skew time in minutes

\[
\text{vserver cifs security modify -vserver vserver_name -kerberos-clock-skew integer_in_minutes}
\]

The default setting is 5 minutes.

Specify the Kerberos ticket lifetime in hours

\[
\text{vserver cifs security modify -vserver vserver_name -kerberos-ticket-age integer_in_hours}
\]

The default setting is 10 hours.

Specify the maximum number of ticket renewal days

\[
\text{vserver cifs security modify -vserver vserver_name -kerberos-renew-age integer_in_days}
\]

The default setting is 7 days.

Specify the timeout for sockets on KDCs after which all KDCs are marked as unreachable

\[
\text{vserver cifs security modify -vserver vserver_name -kerberos-kdc-timeout integer_in_seconds}
\]

The default setting is 3 seconds.

2. Verify the Kerberos security settings:

\[
\text{vserver cifs security show -vserver vserver_name}
\]

**Example**

The following example makes the following changes to Kerberos security: Kerberos Clock Skew is set to 3 minutes and Kerberos Ticket Age is set to 8 hours for SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew 3 -kerberos-ticket-age 8
cluster1::> vserver cifs security show -vserver vs1
Vserver: vs1

<table>
<thead>
<tr>
<th>Kerberos Clock Skew:</th>
<th>3 minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kerberos Ticket Age:</td>
<td>8 hours</td>
</tr>
<tr>
<td>Kerberos Renewal Age:</td>
<td>7 days</td>
</tr>
<tr>
<td>Kerberos KDC Timeout:</td>
<td>3 seconds</td>
</tr>
<tr>
<td>Is Signing Required:</td>
<td>false</td>
</tr>
<tr>
<td>Is Password Complexity Required:</td>
<td>true</td>
</tr>
<tr>
<td>Use start_tls For AD LDAP connection:</td>
<td>false</td>
</tr>
<tr>
<td>Is AES Encryption Enabled:</td>
<td>false</td>
</tr>
<tr>
<td>LM Compatibility Level:</td>
<td>lm-ntlm-ntlmv2-krb</td>
</tr>
<tr>
<td>Is SMB Encryption Required:</td>
<td>false</td>
</tr>
</tbody>
</table>
```

**Related concepts**

- *Kerberos authentication* on page 22
- *Configuring strong security for Kerberos-based communication by using AES encryption* on page 83
- *Supported GPOs* on page 113
- *Applying Group Policy Objects to CIFS servers* on page 113

**Related tasks**

- *Displaying information about CIFS server security settings* on page 79
Setting the CIFS server minimum authentication security level

You can set the CIFS server minimum security level, also known as the *LMCompatibilityLevel*, on your CIFS server to meet your business security requirements for SMB access. The minimum security level is the minimum level of the security tokens that the CIFS server accepts from SMB clients.

**About this task**

You can set the minimum authentication security level to one of four supported security levels:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ntlm-ntlmv2-krb</td>
<td>The SVM accepts NTLM, NTLMv2, and Kerberos authentication security. The SVM denies LM authentication.</td>
</tr>
<tr>
<td>ntlmv2-krb</td>
<td>The SVM accepts NTLMv2 and Kerberos authentication security. The SVM denies LM and NTLM authentication.</td>
</tr>
<tr>
<td>krb</td>
<td>The SVM accepts Kerberos authentication security only. The SVM denies LM, NTLM, and NTLMv2 authentication.</td>
</tr>
</tbody>
</table>

**Steps**

1. Set the minimum authentication security level:
   ```bash
   vserver cifs security modify -vserver vserver_name -lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}
   ```

2. Verify that the authentication security level is set to the desired level:
   ```bash
   vserver cifs security show -vserver vserver_name
   ```

**Related concepts**

*How authentication provides SMB access security* on page 22

**Related tasks**

*Enabling or disabling AES encryption for Kerberos-based communication* on page 84

### Configuring strong security for Kerberos-based communication by using AES encryption

For strongest security with Kerberos-based communication, you can enable AES-256 and AES-128 encryption on the CIFS server. By default, when you create a CIFS server on the Storage Virtual Machine (SVM), AES encryption is disabled. You must enable it to take advantage of the strong security provided by AES encryption.

Kerberos-related communication for CIFS is used during CIFS server creation on the SVM, as well as during the SMB session setup phase. The CIFS server supports the following encryption types for Kerberos communication:

- RC4-HMAC
- DES
- AES 128
• AES 256

If you want to use the highest security encryption type for Kerberos communication, you should enable AES encryption for Kerberos communication on the SVM.

When the CIFS server is created, the domain controller creates a computer machine account in Active Directory. At this time, the KDC becomes aware of the encryption capabilities of the particular machine account. Subsequently, a particular encryption type is selected for encrypting the service ticket that the client presents to the server during authentication.

Related concepts

Kerberos authentication on page 22

Related tasks

Modifying the CIFS server Kerberos security settings on page 81

Enabling or disabling AES encryption for Kerberos-based communication

To take advantage of the strongest security with Kerberos-based communication, you can enable AES-256 and AES-128 encryption on the CIFS server. If you do not want the CIFS server to select the AES encryption types for Kerberos-based communication with the Active Directory (AD) KDC, you can disable AES encryption. By default, AES encryption is disabled.

About this task

To enhance security, the Storage Virtual Machine (SVM) changes its machine account password in the AD each time the AES security option is modified. Changing the password might require administrative AD credentials for the organizational unit (OU) that contains the machine account.

If an SVM is configured as a disaster recovery destination where the identity is not preserved (the –identity-preserve option is set to false in the SnapMirror configuration), the non-default CIFS server security settings are not replicated to the destination. If you have enabled AES encryption on the source SVM, you must manually enable it on the destination SVM after the destination becomes read-write (after the SnapMirror relationship is broken).

Steps

1. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want the AES encryption types for Kerberos communication to be...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>vserver cifs security modify -vserver vserver_name -is-aes-encryption-enabled true</td>
</tr>
<tr>
<td>Disabled</td>
<td>vserver cifs security modify -vserver vserver_name -is-aes-encryption-enabled false</td>
</tr>
</tbody>
</table>

2. Verify that AES encryption is enabled or disabled as desired:

vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled

The is-aes-encryption-enabled field displays true if AES encryption is enabled and false if it is disabled.

Example

The following example enables the AES encryption types for the CIFS server on SVM vs1:
The following example enables the AES encryption types for the CIFS server on SVM vs2. The administrator is prompted to enter the administrative AD credentials for the OU containing the CIFS server.

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes-encryption-enabled true

Info: In order to enable CIFS AES encryption, the password for the CIFS server machine account must be reset. Enter the username and password for the CIFS domain "EXAMPLE.COM".

Enter your user ID: administrator
Enter your password:
```

```
cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-encryption-enabled
vserver  is-aes-encryption-enabled
-------- -------------------------
vs2      true
```

Using SMB signing to enhance network security

SMB signing helps to ensure that network traffic between the CIFS server and the client is not compromised; it does this by preventing replay attacks. By default, Data ONTAP supports SMB signing when requested by the client. Optionally, the storage administrator can configure the CIFS server to require SMB signing.

How SMB signing policies affect communication with a CIFS server

In addition to the CIFS server SMB signing security settings, two SMB signing policies on Windows clients control the digital signing of communications between clients and the CIFS server. You can configure the setting that meets your business requirements.

Client SMB policies are controlled through Windows local security policy settings, which are configured by using the Microsoft Management Console (MMC) or Active Directory GPOs. For more information about client SMB signing and security issues, see the Microsoft Windows documentation.

Here are descriptions of the two SMB signing policies on Microsoft clients:

- **Microsoft network client: Digitally sign communications (if server agrees)**
  This setting controls whether the client’s SMB signing capability is enabled. It is enabled by default. When this setting is disabled on the client, the client communications with the CIFS server will depend on the SMB signing setting on the CIFS server.

- **Microsoft network client: Digitally sign communications (always)**
  This setting controls whether the client requires SMB signing to communicate with a server. It is disabled by default. When this setting is disabled on the client, SMB signing behavior is based on the policy setting for **Microsoft network client: Digitally sign communications (if server agrees)** and the setting on the CIFS server.
**Note:** If your environment includes Windows clients configured to require SMB signing, you must enable SMB signing on the CIFS server. If you do not, the CIFS server cannot serve data to these systems.

The effective results of client and CIFS server SMB signing settings depends on whether the SMB sessions uses SMB 1.0 or SMB 2.x and later.

The following table summarizes the effective SMB signing behavior if the session uses SMB 1.0:

<table>
<thead>
<tr>
<th>Client</th>
<th>Data ONTAP—signing not required</th>
<th>Data ONTAP—signing required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signing disabled and not required</td>
<td>Not signed</td>
<td>Signed</td>
</tr>
<tr>
<td>Signing enabled and not required</td>
<td>Not signed</td>
<td>Signed</td>
</tr>
<tr>
<td>Signing disabled and required</td>
<td>Signed</td>
<td>Signed</td>
</tr>
<tr>
<td>Signing enabled and required</td>
<td>Signed</td>
<td>Signed</td>
</tr>
</tbody>
</table>

**Note:**

Older Windows SMB 1 clients and some non-Windows SMB 1 clients might fail to connect if signing is disabled on the client but required on the CIFS server.

The following table summarizes the effective SMB signing behavior if the session uses SMB 2.x or SMB 3.0:

**Note:** For SMB 2.x and SMB 3.0 clients, SMB signing is always enabled. It cannot be disabled.

<table>
<thead>
<tr>
<th>Client</th>
<th>Data ONTAP—signing not required</th>
<th>Data ONTAP—signing required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signing not required</td>
<td>Not signed</td>
<td>Signed</td>
</tr>
<tr>
<td>Signing required</td>
<td>Signed</td>
<td>Signed</td>
</tr>
</tbody>
</table>

The following table summarizes the default Microsoft client and server SMB signing behavior:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Hash algorithm</th>
<th>Can enable/disable</th>
<th>Can require/not require</th>
<th>Client default</th>
<th>Server default</th>
<th>DC default</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMB 1.0</td>
<td>MD5</td>
<td>Yes</td>
<td>Yes</td>
<td>Enabled (not required)</td>
<td>Disabled (not required)</td>
<td>Required</td>
</tr>
<tr>
<td>SMB 2.x</td>
<td>HMAC-SHA-256</td>
<td>No</td>
<td>Yes</td>
<td>Not required</td>
<td>Not required</td>
<td>Required</td>
</tr>
<tr>
<td>SMB 3.0</td>
<td>AES-CMAC.</td>
<td>No</td>
<td>Yes</td>
<td>Not required</td>
<td>Not required</td>
<td>Required</td>
</tr>
</tbody>
</table>

**Note:** Microsoft no longer recommends using **Digitally sign communications (if client agrees)** or **Digitally sign communications (if server agrees)** Group Policy settings. Microsoft also no longer recommends using the **EnableSecuritySignature** registry settings. These options only affect the SMB 1 behavior and can be replaced by the **Digitally sign communications (always)** Group Policy setting or the **RequireSecuritySignature** registry setting. For more information, see the Microsoft Blog *The Basics of SMB Signing (covering both SMB1 and SMB2).*
Performance impact of SMB signing

When SMB sessions use SMB signing, all SMB communications to and from Windows clients experience a significant impact on performance, which affects both the clients and the server (that is, the nodes on the cluster running the Storage Virtual Machine (SVM) containing the CIFS server).

The performance degradation shows as increased CPU usage on both the clients and the server, although the amount of network traffic does not change.

Depending on your network and SVM implementation, the performance impact of SMB signing can vary widely; you can verify it only through testing in your network environment.

Most Windows clients negotiate SMB signing by default if it is enabled on the server. If you require SMB protection for some of your Windows clients, and if SMB signing is causing performance issues, you can disable SMB signing on any of your Windows clients that do not require protection against replay attacks. For information about disabling SMB signing on Windows clients, see the Microsoft Windows documentation.

Recommendations for configuring SMB signing

You can configure SMB signing behavior between SMB clients and the CIFS server to meet your security requirements. The settings you choose when configuring SMB signing on your CIFS server are dependent on what your security requirements are.

You can configure SMB signing on either the client or the CIFS server. Consider the following recommendations when configuring SMB signing:

<table>
<thead>
<tr>
<th>If...</th>
<th>Recommendation...</th>
</tr>
</thead>
<tbody>
<tr>
<td>You want to increase the security of the communication between the client and the server</td>
<td>Make SMB signing required at the client by enabling the Require Option (Sign always) security setting on the client.</td>
</tr>
<tr>
<td>You want all SMB traffic to a certain Storage Virtual Machine (SVM) signed</td>
<td>Make SMB signing required on the CIFS server by configuring the security settings to require SMB signing.</td>
</tr>
</tbody>
</table>

See Microsoft documentation for more information on configuring Windows client security settings.

Related tasks

*Enabling or disabling required SMB signing for incoming SMB traffic*

Considerations when multiple data LIFS are configured

If you enable or disable required SMB signing on the CIFS sever, there are certain considerations you should keep in mind when you have multiple data LIFS configured for a Storage Virtual Machine (SVM).

When you configure a CIFS server, there might be multiple data LIFS configured. If so, the DNS server contains multiple A record entries for the CIFS server, all using the same CIFS server host name, but each with a unique IP address. For example, a CIFS server that has two data LIFS configured might have the following DNS A record entries:

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

The normal behavior is that upon changing the required SMB signing setting, only new connections from clients are affected by the change in the SMB signing setting. However, there is an exception to this behavior. There is a case where a client has an existing connection to a share, and the client creates a new connection to the same share after the setting is changed, while maintaining the
original connection. In this case, both the new and the existing SMB connection adopt the new SMB signing requirements.

Consider the following example:

1. Client1 connects to a share without required SMB signing using the path `O: \`
2. The storage administrator modifies the CIFS server configuration to require SMB signing.
3. Client1 connects to the same share with required SMB signing using the path `S: \` (while maintaining the connection using the path `O: \`).
4. The result is that SMB signing is used when accessing data over both the `O: \` and `S: \` drives.

**Enabling or disabling required SMB signing for incoming SMB traffic**

You can enforce the requirement for clients to sign SMB messages by enabling required SMB signing. If enabled, Data ONTAP accepts SMB messages only if they have valid signatures. If you want to permit SMB signing, but not require it, you can disable required SMB signing.

**About this task**

By default, required SMB signing is disabled. You can enable or disable required SMB signing at any time.

**Note:** SMB signing is not disabled by default under the following circumstance:

1. Required SMB signing is enabled and the cluster is reverted to a version of Data ONTAP that does not support SMB signing.
2. The cluster is subsequently upgraded to a version of Data ONTAP that supports SMB signing. Under these circumstances, the SMB signing configuration originally configured on a supported version of Data ONTAP is retained through reversion and subsequent upgrade.

When you set up a Storage Virtual Machine (SVM) disaster recovery relationship, the value you select for the `-identity-preserve` option of the `snapmirror create` command determines the configuration details that are replicated in the destination SVM.

If you set the `-identity-preserve` option to `true` (ID-preserve), the SMB signing security setting is replicated to the destination.

If you set the `-identity-preserve` option to `false` (non-ID-preserve), the SMB signing security setting is not replicated to the destination. In this case, the CIFS server security settings on the destination are set to the default values. If you have enabled required SMB signing on the source SVM, you must manually enable required SMB signing on the destination.

**Steps**

1. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want required SMB signing to be...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td><code>vserver cifs security modify -vserver vserver_name -is-signing-required true</code></td>
</tr>
<tr>
<td>Disabled</td>
<td><code>vserver cifs security modify -vserver vserver_name -is-signing-required false</code></td>
</tr>
</tbody>
</table>

2. Verify that required SMB signing is enabled or disabled by determining if the value in the Is Signing Required field in the output from the following command is set to the desired value:
**Example**

The following example enables required SMB signing for Storage Virtual Machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required true
cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-required
vserver is-signing-required
-------- -------------------
vs1      true
```

**Determining whether SMB sessions are signed**

You can display information about connected SMB sessions on the CIFS server. You can use this information to determine whether SMB sessions are signed. This can be helpful in determining whether SMB client sessions are connecting with the desired security settings.

**Step**

1. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want display information about...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>All signed sessions on a specified Storage Virtual Machine (SVM)</td>
<td><code>vserver cifs session show -vserver vserver_name -is-session-signed true</code></td>
</tr>
<tr>
<td>Details for a signed session with a specific session ID on the SVM</td>
<td><code>vserver cifs session show -vserver vserver_name -session-id integer -instance</code></td>
</tr>
</tbody>
</table>

**Examples**

The following command displays session information about signed sessions on SVM vs1. The default summary output does not display the “Is Session Signed” output field:

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node: nodel
Vserver: vs1
Connection Session ID Workstation Windows User Open Files Idle
------- --------- --------------- --------- ------- --------
3151272279 10.1.1.1 DOMAIN\joe 2
```

The following command displays detailed session information, including whether the session is signed, on an SMB session with a session ID of 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node: nodel
Vserver: vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\joe
UNIX User: pcuser
Open Shares: 1
```
Related tasks

Enabling or disabling required SMB signing for incoming SMB traffic
Monitoring SMB signed session statistics on page 90

Monitoring SMB signed session statistics

You can monitor SMB sessions statistics and determine which established sessions are signed and which are not.

About this task

The `statistics` command at the advanced privilege level provides the `signed_sessions` counter that you can use to monitor the number of signed SMB sessions. The `signed_sessions` counter is available with the following statistics objects:

- `cifs` enables you to monitor SMB signing for all SMB sessions.
- `smb1` enables you to monitor SMB signing for SMB 1.0 sessions.
- `smb2` enables you to monitor SMB signing for SMB 2.x and SMB 3.0 sessions.

Note: SMB 3.0 statistics are included in the output for the `smb2` object.

If you want to compare the number of signed session to the total number of sessions, you can compare output for the `signed_sessions` counter with the output for the `established_sessions` counter.

You must start a statistics sample collection before you can view the resultant data. You can view data from the sample if you do not stop data collection. Stopping data collection gives you a fixed sample. Not stopping data collection gives you the ability to get updated data that you can use to compare against previous queries. The comparison can help you identify trends.

For more information about using the `statistics` command, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators.*

Steps

1. Set the privilege level to advanced:
   ```
   set -privilege advanced
   ```

2. Start a data collection:
   ```
   statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]
   ```

   If you do not specify the `-sample-id` parameter, the command generates a sample identifier for you and defines this sample as the default sample for the CLI session. The value for `-sample-id` is a text string. If you run this command during the same CLI session and do not specify the `-sample-id` parameter, the command overwrites the previous default sample.
You can optionally specify the node on which you want to collect statistics. If you do not specify the node, the sample collects statistics for all nodes in the cluster.

3. Optional: Use the `statistics stop` command to stop collecting data for the sample.

4. View SMB signing statistics:

   If you want to view information for...
   Enter...

   | Signed sessions | `show -sample-id sample_ID -counter signed_sessions|node_name [...]` |
   | Signed sessions and established sessions | `show -sample-id sample_ID -counter signed_sessions|established_sessions|node_name [...]` |

   If you want to display information for only a single node, specify the optional `-node node_name` parameter.

5. Return to the admin privilege level:

   `set -privilege admin`

**Examples**

The following example shows how you can monitor SMB 2.x and SMB 3.0 signing statistics on Storage Virtual Machine (SVM) vs1.

The following command moves to the advanced privilege level:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

The following command starts data collection for a new sample:

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample -vserver vs1
Statistics collection is being started for Sample-id: smbsigning_sample
```

The following command stops the data collection for the sample:

```
cluster1::*> statistics stop -sample-id smbsigning_sample
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

The following command shows signed SMB sessions and established SMB sessions by node from the sample:

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter signed_sessions|established_sessions|node_name
```

<table>
<thead>
<tr>
<th>Object: smb2</th>
<th>Instance: vs1</th>
<th>Start-time: 2/6/2013 01:00:00</th>
<th>End-time: 2/6/2013 01:03:04</th>
<th>Cluster: cluster1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Counter</td>
<td>Value</td>
<td>-----------------------------</td>
<td>-----------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>established_sessions</td>
<td>0</td>
<td>node_name</td>
<td>node1</td>
<td>signed_sessions</td>
</tr>
</tbody>
</table>
established_sessions         1
node_name                    node2
signed_sessions              1
established_sessions         0
node_name                    node3
signed_sessions              0
established_sessions         0
node_name                    node4
signed_sessions              0

The following command shows signed SMB sessions for node2 from the sample:

cluster1::*> statistics show -sample-id smbsigning_sample -counter signed_sessions|node_name -node node2

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:22:43
Cluster: cluster1

<table>
<thead>
<tr>
<th>Counter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>node_name</td>
<td>node2</td>
</tr>
<tr>
<td>signed_sessions</td>
<td>1</td>
</tr>
</tbody>
</table>

The following command moves back to the admin privilege level:

cluster1::*> set -privilege admin

Related tasks

* Enabling or disabling required SMB signing for incoming SMB traffic
* Determining whether SMB sessions are signed on page 89

Configuring required SMB encryption on CIFS servers for data transfers over SMB

SMB encryption for data transfers over SMB is a security enhancement that you can enable or disable on CIFS servers. After it is enabled, you can configure the desired SMB encryption setting on a share-by-share basis through a share property setting.

By default, when you create a CIFS server on the Storage Virtual Machine (SVM), SMB encryption is disabled. You must enable it to take advantage of the enhanced security provided by SMB encryption.

To create an encrypted SMB session, the SMB client must support SMB encryption. Windows clients starting with Windows Server 2012 and Windows 8 support SMB encryption.

SMB encryption on the SVM is controlled through two settings:

- A CIFS server security option that enables the functionality on the SVM
- A CIFS share property that configures the SMB encryption setting on a share-by-share basis

You can decide whether to require encryption for access to all data on the SVM or to require SMB encryption to access data only in selected shares. SVM-level settings supersede share-level settings.

The effective SMB encryption configuration depends on the combination of the two settings and is described in the following table:
CIFS server SMB encryption enabled | Share encrypt data setting enabled | Server-side encryption behavior
--- | --- | ---
True | False | Server-level encryption is enabled for all of the shares in the SVM. With this configuration, encryption happens for the entire SMB session.
True | True | Server-level encryption is enabled for all of the shares in the SVM irrespective of share-level encryption. With this configuration, encryption happens for the entire SMB session.
False | True | Share-level encryption is enabled for the specific shares. With this configuration, encryption happens from the tree connect.
False | False | No encryption is enabled.

SMB clients that do not support encryption cannot connect to a CIFS server or share that requires encryption.

**Enabling or disabling required SMB encryption for incoming SMB traffic**

If you want to require SMB encryption for incoming SMB traffic you can enable it on the CIFS server or at the share level. By default, SMB encryption is not required.

**About this task**

You can enable SMB encryption on the CIFS server, which applies to all shares on the CIFS server. If you do not want required SMB encryption for all shares on the CIFS server or if you want to enable required SMB encryption for incoming SMB traffic on a share-by-share basis, you can disable required SMB encryption on the CIFS server.

When you set up a Storage Virtual Machine (SVM) disaster recovery relationship, the value you select for the `identity-preserve` option of the `snapmirror create` command determines the configuration details that are replicated in the destination SVM.

If you set the `identity-preserve` option to `true` (ID-preserve), the SMB encryption security setting is replicated to the destination.

If you set the `identity-preserve` option to `false` (non-ID-preserve), the SMB encryption security setting is not replicated to the destination. In this case, the CIFS server security settings on the destination are set to the default values. If you have enabled SMB encryption on the source SVM, you must manually enable CIFS server SMB encryption on the destination.

**Steps**

1. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want required SMB encryption for incoming SMB traffic on the CIFS server to be...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td><code>vserver cifs security modify -vserver vserver_name -is-smb-encryption-required true</code></td>
</tr>
</tbody>
</table>
If you want required SMB encryption for incoming SMB traffic on the CIFS server to be...

<table>
<thead>
<tr>
<th>Disabled</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>vserver cifs security modify -vserver vserver_name -is-smb-encryption-required false</td>
<td></td>
</tr>
</tbody>
</table>

2. Verify that required SMB encryption on the CIFS server is enabled or disabled as desired:

vserver cifs security show -vserver vserver_name -fields is-smb-encryption-required

The is-smb-encryption-required field displays true if required SMB encryption is enabled on the CIFS server and false if it is disabled.

Example

The following example enables required SMB encryption for incoming SMB traffic for the CIFS server on SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-encryption-required

vserver is-smb-encryption-required
-------- -------------------------
vs1      true
```

Determining whether clients are connected using encrypted SMB sessions

You can display information about connected SMB sessions to determine whether clients are using encrypted SMB connections. This can be helpful in determining whether SMB client sessions are connecting with the desired security settings.

About this task

SMB clients sessions can have one of three encryption levels:

- **unencrypted**
  The SMB session is not encrypted. Neither Storage Virtual Machine (SVM)-level or share-level encryption is configured.

- **partially-encrypted**
  Encryption is initiated when the tree-connect occurs. Share-level encryption is configured. SVM-level encryption is not enabled.

- **encrypted**
  The SMB session is fully encrypted. SVM-level encryption is enabled. Share level encryption might or might not be enabled. The SVM-level encryption setting supersedes the share-level encryption setting.

Step

1. Perform one of the following actions:
If you want to display information about...

Enter the command...

Sessions with a specified encryption setting for sessions on a specified SVM

`vserver cifs session show -vserver vserver_name (unencrypted|partially-encrypted|encrypted) -instance`

The encryption setting for a specific session ID on a specified SVM

`vserver cifs session show -vserver vserver_name -session-id integer -instance`

Examples

The following command displays detailed session information, including the encryption setting, on an SMB session with a session ID of 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node: node1
Vserver: vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\joe
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: CIFS_ALIAS1
SMB Encryption Status: Unencrypted
```

Using LDAP over SSL/TLS to secure communication

You can use LDAP over SSL/TLS to secure communication between the Storage Virtual Machine (SVM) LDAP client and the LDAP server. This allows LDAP to encrypt all traffic to and from the LDAP server.

LDAP over SSL/TLS concepts

You must understand certain terms and concepts about how Data ONTAP uses SSL/TLS to secure LDAP communication. Data ONTAP can use LDAP over SSL/TLS for setting up authenticated sessions between Active Directory-integrated LDAP servers or UNIX-based LDAP servers.

Terminology

There are certain terms that you should understand about how Data ONTAP uses LDAP over SSL to secure LDAP communication.

LDAP

(Lightweight Directory Access Protocol) A protocol for accessing and managing information directories. LDAP is used as an information directory for storing objects such as users, groups, and netgroups. LDAP also provides directory services that manage these objects and fulfill LDAP requests from LDAP clients.

SSL
(Secure Sockets Layer) A secure protocol developed for sending information securely over the Internet. SSL is used to provide either server or mutual (server and client) authentication. SSL provides encryption only. If a method to ensure data integrity is needed, it must be provided by the application using SSL.

TLS
(Transport Layer Security) An IETF standards track protocol that is based on the earlier SSL specifications. It is the successor to SSL.

LDAP over SSL/TLS
(Also known as LDAPS) A protocol that uses SSL or TLS to secure communication between LDAP clients and LDAP servers. The terms SSL and TLS are often used interchangeably unless referring to a specific version of the protocol.

Start TLS
(Also known as start_tls, STARTTLS, and StartTLS) A mechanism to provide secure communication by using the TLS/SSL protocols.

How Data ONTAP uses LDAP over SSL/TLS
By default, LDAP communications between client and server applications are not encrypted. This means that it is possible to use a network monitoring device or software and view the communications between LDAP client and server computers. This is especially problematic when an LDAP simple bind is used because the credentials (user name and password) used to bind the LDAP client to the LDAP server are passed over the network unencrypted.

The SSL and TLS protocols run above TCP/IP and below higher-level protocols, such as LDAP. They use TCP/IP on behalf of the higher-level protocols, and in the process, permit an SSL-enabled server to authenticate itself to an SSL-enabled client and permit both machines to establish an encrypted connection. These capabilities address fundamental security concerns about communication over the Internet and other TCP/IP networks.

Data ONTAP supports SSL server authentication, which enables the Storage Virtual Machine (SVM) LDAP client to confirm the LDAP server’s identity during the bind operation. SSL/TLS-enabled LDAP clients can use standard techniques of public-key cryptography to check that a server’s certificate and public ID are valid and have been issued by a certificate authority (CA) listed in the client’s list of trusted CAs.

This version of Data ONTAP supports the following:

- LDAP over SSL/TLS for SMB-related traffic between the Active Directory-integrated LDAP servers and the SVM
- LDAP over SSL/TLS for LDAP traffic for name mapping
  Either Active Directory-integrated LDAP servers or UNIX-based LDAP servers can be used to store information for LDAP name mapping.
- Self-signed root CA certificates
  When using an Active-Directory integrated LDAP, the self-signed root certificate is generated when the Windows Server Certificate Service is installed in the domain. When using an UNIX-based LDAP server for LDAP name mapping, the self-signed root certificate is generated and saved by using means appropriate to that LDAP application.

Data ONTAP does not support signing (integrity protection) and sealing (encryption) of the data.

By default, LDAP over SSL/TLS is disabled.

Data ONTAP uses port 389 for LDAP over SSL/TLS
LDAP supports two methods to encrypt communications using SSL/TLS: traditional LDAPS and STARTTLS. LDAPS communication usually occurs over a special port, commonly 636. However,
STARTTLS begins as a plaintext connection over the standard LDAP port (389), and that connection is then upgraded to SSL/TLS.

Data ONTAP uses STARTTLS for securing LDAP communication, and uses the default LDAP port (389) to communicate with the LDAP server. LDAP over SSL/TLS on the SVM should not be configured to use port 636 because this causes LDAP connections to fail. The LDAP server must be configured to allow connections over LDAP port 389; otherwise, LDAP SSL/TLS connections from the SVM to the LDAP server fail.

Configuring LDAP over SSL/TLS

To configure LDAP over SSL/TLS, you must enable LDAP over SSL/TLS on the Storage Virtual Machine (SVM), export a copy of the self-signed root CA certificate, and, using the exported file, install the self-signed root CA certificate on the SVM.

Steps

1. **Enabling LDAP over SSL/TLS on the CIFS server** on page 97
   Before your CIFS server can use secure LDAP communication to an Active Directory LDAP server, you must modify the CIFS server security settings to enable LDAP over SSL/TLS for Active Directory server LDAP communication.

2. **Exporting a copy of the self-signed root CA certificate** on page 98
   To use LDAP over SSL/TLS for securing Active Directory communication, you must first export a copy of the Active Directory Certificate Service's self-signed root CA certificate to a certificate file and convert it to an ASCII text file. This text file is used by Data ONTAP to install the certificate on the Storage Virtual Machine (SVM).

3. **Installing the self-signed root CA certificate on the SVM** on page 98
   Before you can use secure LDAP authentication when binding to LDAP servers, you must install the self-signed root CA certificate on the Storage Virtual Machine (SVM).

Related information

*Clustered Data ONTAP 8.3 System Administration Guide*

**Enabling LDAP over SSL/TLS on the CIFS server**

Before your CIFS server can use secure LDAP communication to an Active Directory LDAP server, you must modify the CIFS server security settings to enable LDAP over SSL/TLS for Active Directory server LDAP communication.

Steps

1. Configure the CIFS server security setting that allows secure LDAP communication with Active Directory LDAP servers:
   ```
   vserver cifs security modify -vserver vserver_name -use-start-tls-for-ad-ldap true
   ```

2. Verify that the LDAP over SSL/TLS security setting is set to **true**:
   ```
   vserver cifs security show -vserver vserver_name
   ```

After you finish

Install the self-signed root CA certificate that you exported from the Certificate Service certificate store on the Storage Virtual Machine (SVM).

If you have the LDAP client configured on the SVM, for example, if the SVM is multiprotocol or if you are using LDAP for user-mapping and you want to enable LDAP over SSL on the LDAP client, you can enable it by using the `vserver services name-service ldap client create` or
vserver services name-service ldap client modify commands with the -use-start-tls option set to true.

For more information about creating an LDAP client configuration, see the Clustered Data ONTAP File Access Management Guide for NFS.

Exporting a copy of the self-signed root CA certificate

To use LDAP over SSL/TLS for securing Active Directory communication, you must first export a copy of the Active Directory Certificate Service's self-signed root CA certificate to a certificate file and convert it to an ASCII text file. This text file is used by Data ONTAP to install the certificate on the Storage Virtual Machine (SVM).

Before you begin

The Active Directory Certificate Service must already be installed and configured for the domain to which the CIFS server belongs. You can find information about installing and configuring Active Director Certificate Services by consulting the Microsoft TechNet Library: technet.microsoft.com.

Step

1. Obtain a root CA certificate of the domain controller that is in the .pem text format.

   For more information, consult the Microsoft TechNet Library: technet.microsoft.com.

After you finish

Install the certificate on the SVM.

Related information

Microsoft TechNet Library

Installing the self-signed root CA certificate on the SVM

Before you can use secure LDAP authentication when binding to LDAP servers, you must install the self-signed root CA certificate on the Storage Virtual Machine (SVM).

About this task

When LDAP over SSL/TLS is enabled, the Data ONTAP LDAP client on the SVM does not support revoked certificates. The LDAP client treats revoked certificates as if they are not revoked.

Steps

1. Install the self-signed root CA certificate:

   a. Begin the certificate installation:

      ```
      security certificate install -vserver vserver_name -type server-ca
      ```

      The console output displays the following message:

      Please enter Certificate: Press <Enter> when done

   b. Open the certificate .pem file with a text editor, copy the certificate, including the lines beginning with -----BEGIN CERTIFICATE----- and ending with -----END CERTIFICATE-----, and then paste the certificate on the console.

   c. Verify that the certificate is displayed after the console prompt.

   d. Complete the installation by pressing Enter.

2. Verify that the certificate is installed:
Confi guring default Windows user to UNIX user mappings on the CIFS server

For Windows (SMB) users that do not map to a specific user in the configured UNIX user directory stores (either by using implicit name mapping or by explicitly confi guring a Windows to UNIX user name mapping), you can confi gure default Windows user to UNIX user mappings on the CIFS server.

- SMB users receive UNIX credentials by confi guring a default UNIX account (for local SMB user accounts and domain users from the home domain or trusted domains).
- SMB users receive UNIX credentials by confi guring a guest UNIX account (for users connecting from non-local accounts or users from non-trusted domains).
- The home domain’s Domain Administrators group receive the root account UNIX credentials by enabling a CIFS server option.

Confi guring the default UNIX user

You can confi gure the default UNIX user to use if all other mapping attempts fail for a user, or if you do not want to map individual users between UNIX and Windows. Alternatively, if you want authentication of non-mapped users to fail, you should not confi gure the default UNIX user.

About this task

By default, the name of the default UNIX user is “pcuser”, which means that, by default, user mapping to the default UNIX user is enabled. You can specifi c another name to use as the default UNIX user. The name that you specify must exist in the name service databases confi gured for the Storage Virtual Machine (SVM). If this option is set to a null string, no one can access the CIFS server as a UNIX default user. That is, each user must have an account in the password database before they can access the CIFS server.

For a user to connect to the CIFS server using the default UNIX user account, the user must meet the following prerequisites:

- The user is authenticated.
- The user is in the CIFS server’s local Windows user database, in the CIFS server’s home domain, or in a trusted domain (if multidomain name mapping searches is enabled on the CIFS server).
- The user name is not explicitly mapped to a null string.

Steps

1. Configure the default UNIX user:

<table>
<thead>
<tr>
<th>If you want to …</th>
<th>Enter …</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the default UNIX user “pcuser”</td>
<td><code>vserver cifs options modify -default-unix-user pcuser</code></td>
</tr>
<tr>
<td>Use another UNIX user account as the default user</td>
<td><code>vserver cifs options modify -default-unix-user user_name</code></td>
</tr>
<tr>
<td>Disable the default UNIX user</td>
<td><code>vserver cifs options modify -default-unix-user &quot;&quot;</code></td>
</tr>
</tbody>
</table>

Example

`vserver cifs options modify -default-unix-user pcuser`
2. Verify that the default UNIX user is configured correctly:

   vserver cifs options show -vserver vserver_name

**Example**

In the following example, both the default UNIX user and the guest UNIX user on SVM vs1 are configured to use UNIX user “pcuser”:

   vserver cifs options show -vserver vs1

```
Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : pcuser
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

**Related concepts**

- [Creating name mappings](#) on page 163
- [How name mapping is used to secure SMB file access on SVMs with FlexVol volumes](#) on page 23

### Configuring the guest UNIX user

Configuring the guest UNIX user option means that users who log in from untrusted domains are mapped to the guest UNIX user and can connect to the CIFS server. Alternatively, if you want authentication of users from untrusted domains to fail, you should not configure the guest UNIX user. The default is to not allow users from untrusted domains to connect to the CIFS server (the guest UNIX account is not configured).

**About this task**

You should keep the following in mind when configuring the guest UNIX account:

- If the CIFS server cannot authenticate the user against a domain controller for the home domain or a trusted domain or the local database and this option is enabled, the CIFS server considers the user as a guest user and maps the user to the specified UNIX user.
- If this option is set to a null string, the guest UNIX user is disabled.
- You must create a UNIX user to use as the guest UNIX user in one of the Storage Virtual Machine (SVM) name service databases.
- A user logged in as a guest user is automatically a member of the BUILTIN\guests group on the CIFS server.
- A user logged in as a guest user does not have a home directory.

**Steps**

1. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Enter...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the guest UNIX user</td>
<td>vserver cifs options modify -guest-unix-user unix_name</td>
</tr>
<tr>
<td>Disable the guest UNIX user</td>
<td>vserver cifs options modify -guest-unix-user &quot;&quot;</td>
</tr>
</tbody>
</table>
Example

`vserver cifs options modify -guest-unix-user pcuser`

2. Verify that the guest UNIX user is configured correctly:

`vserver cifs options show -vserver vserver_name`

Example

In the following example, both the default UNIX user and the guest UNIX user on SVM vs1 are configured to use UNIX user “pcuser”:

`vserver cifs options show -vserver vs1`

<table>
<thead>
<tr>
<th>Vserver: vs1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Session Timeout : 900</td>
</tr>
<tr>
<td>Default Unix Group : -</td>
</tr>
<tr>
<td>Default Unix User : pcuser</td>
</tr>
<tr>
<td>Guest Unix User : pcuser</td>
</tr>
<tr>
<td>Read Grants Exec : disabled</td>
</tr>
<tr>
<td>Read Only Delete : disabled</td>
</tr>
<tr>
<td>WINS Servers : -</td>
</tr>
</tbody>
</table>

Mapping the administrators group to root

If you have only CIFS clients in your environment and your Storage Virtual Machine (SVM) was set up as a multiprotocol storage system, you must have at least one Windows account that has root privilege for accessing files on the SVM; otherwise, you cannot manage the SVM because you do not have sufficient user rights.

About this task

If your storage system was set up as NTFS-only, however, the `/etc` directory has a file-level ACL that enables the administrators group to access the Data ONTAP configuration files.

Steps

1. Set the privilege level to advanced:

   `set -privilege advanced`

2. Configure the CIFS server option that maps the administrators group to root as appropriate:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map the administrator group members to root</td>
<td><code>vserver cifs options modify -vserver vserver_name -is-admin-users-mapped-to-root-enabled true</code></td>
</tr>
<tr>
<td></td>
<td>All accounts in the administrators group are considered root, even if you do not have an <code>/etc/usermap.cfg</code> entry mapping the accounts to root. If you create a file using an account that belongs to the administrators group, the file is owned by root when you view the file from a UNIX client.</td>
</tr>
<tr>
<td>Disable mapping the administrators group members to root</td>
<td><code>vserver cifs options modify -vserver vserver_name -is-admin-users-mapped-to-root-enabled false</code></td>
</tr>
<tr>
<td></td>
<td>Accounts in the administrators group no longer map to root. You can only explicitly map a single user to root.</td>
</tr>
</tbody>
</table>

3. Verify that the option is set to the desired value:

   `vserver cifs options show -vserver vserver_name`
4. Return to the admin privilege level:
   set -privilege admin

Displaying information about what types of users are connected over SMB sessions

You can display information about what type of users are connected over SMB sessions. This can help you ensure that only the appropriate type of user is connecting over SMB sessions on the Storage Virtual Machine (SVM).

About this task

The following types of users can connect over SMB sessions:

- **local-user**
  Authenticated as a local CIFS user

- **domain-user**
  Authenticated as a domain user (either from the CIFS server's home domain or a trusted domain)

- **guest-user**
  Authenticated as a guest user

- **anonymous-user**
  Authenticated as an anonymous or null user

Step

1. Determine what type of user is connected over an SMB session:

   vserver cifs session show -vserver vserver_name -windows-user windows_user_name -fields windows-user,address,lif-address,user-type

<table>
<thead>
<tr>
<th>If you want to display user type information for established sessions...</th>
<th>Enter the following command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>For all sessions with a specified user type</td>
<td>vserver cifs session show -vserver vserver_name -user-type {local-user</td>
</tr>
<tr>
<td>For a specific user</td>
<td>vserver cifs session show -vserver vserver_name -windows-user windows_user_name -fields windows-user,address,lif-address,user-type</td>
</tr>
</tbody>
</table>

Examples

The following command displays session information on the user type for sessions on SVM vs1 established by user “iepubs\user1”:

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user iepubs\user1 -node node1 -fields windows-user,address,lif-address,user-type
windows-user user-type windows-session-id connection-id lif-address address
------------- -------- --------------------------- ------------------------
IEPUBS domain-user 3439441860 10.0.0.1 10.1.1.1
```
Configuring SMB on your CIFS server

Server Message Block (SMB) is a remote file-sharing protocol used by Microsoft Windows clients and servers. You can configure and manage SMB on the CIFS server associated with your Storage Virtual Machine (SVM).

Related concepts

*Using SMB signing to enhance network security* on page 85

Supported SMB versions

Data ONTAP supports several versions of the Server Message Block (SMB) protocol on your CIFS server on the data SVM. Data ONTAP support for SMB for SVMs with FlexVol volumes and SVMs with Infinite Volumes differ. You need to be aware of which versions are supported for each type of Storage Virtual Machine (SVM).

Data ONTAP supports the following SMB versions for SVMs with FlexVol volumes and SVMs with Infinite Volumes:

<table>
<thead>
<tr>
<th>SMB version</th>
<th>Supported on SVMs with FlexVol volumes?</th>
<th>Supported on SVMs with Infinite Volumes?</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMB 1.0</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SMB 2.0</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>SMB 2.1</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>SMB 3.0</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Supported SMB 1.0 functionality**

The CIFS (SMB 1.0) protocol was introduced by Microsoft for Windows clients. Data ONTAP supports the SMB 1.0 protocol on all versions of clustered Data ONTAP and on Storage Virtual Machines (SVMs) with FlexVol volumes and SVMs with Infinite Volumes.

Over the years, Microsoft has extended the original SMB 1.0 protocol with enhancements to security, file, and disk-management features. Legacy Windows clients (pre-Windows XP) or non-Windows clients that support only SMB 1.0 can access data on the SVM using SMB 1.0.

**Supported SMB 2.0 functionality**

Clustered Data ONTAP 8.1 and later supports the SMB 2.0 protocol on Storage Virtual Machines (SVMs) with FlexVol volumes. SMB 2.0 is a major redesign of the SMB protocol that provides performance enhancements and added resiliency against network interruptions through the use of durable handles.

SMB 2.0 is enabled automatically when you create a CIFS server.

Data ONTAP supports the following SMB 2.0 functionality:

- **Durable handles**
  Enables clients to transparently reconnect to disconnected SMB sessions after short network outages. For example, LIF failovers, LIF moves, and LIF migrations are transparent and nondisruptive for SMB 2.0 connections.

- **Compounded operations**
  Provides a method for combining multiple SMB messages into a single network transmission request for submission to the underlying transport.
• Asynchronous operations
  Certain SMB commands from the clients can take a longer time for the server to process. For these commands, the CIFS server can send responses asynchronously.

• Increased read and write buffer sizes
  Allows for better throughput across faster networks, even those with high latency.

• Increased scalability
  SMB 2.0 has increased limits for number of SMB sessions, open share connections, and open file connections.

• Increased SMB signing security
  Support for stronger data integrity protection through the use of the HMAC-SHA256 hash algorithm.

Data ONTAP does not support the following SMB 2.0 functionality:

• Symbolic links
• Credit system for flow control

If SMB 2.0 is disabled on the CIFS server, communication between the SMB 2.0 client and the CIFS server falls back to the SMB 1.0 protocol (assuming that the SMB 2.0 client includes the SMB 1.0 dialect in its negotiate request).

For more information, see Technical Report TR-3740 or the SMB 2.0 protocol specification.

Related information

Supported SMB 2.1 functionality

The SMB 2.1 protocol provides several enhancements to the SMB 2.0 protocol. Data ONTAP 8.1 and later supports SMB 2.1 on Storage Virtual Machines (SVMs) with FlexVol volumes. Support for SMB 2.1 is enabled automatically when you enable the SMB 2.0 protocol on the CIFS server.

SMB 2.0 and SMB 2.1 are enabled automatically when you create a CIFS server. SMB 2.0 and SMB 2.1 are always enabled or disabled together. You cannot enable or disable SMB 2.0 and SMB 2.1 separately.

Data ONTAP supports the following SMB 2.1 functionality:

• Lease oplocks
  Data ONTAP uses SMB 2.1 lease oplocks, which is a new client oplock leasing model that provides advantages over traditional oplocks. Lease oplocks offer more flexibility and levels in controlling the client caching. This results in significant performance improvement in high-latency and erratic networks.

• BranchCache version 1
  BranchCache is a feature that delivers WAN bandwidth optimization and improved file access performance using client-side caching at remote offices. SMB 2.1 has the functional extensions needed to manage content hashes, which are used by BranchCache-enabled CIFS servers to provide clients with information about cached content.

Data ONTAP does not support the following SMB 2.1 functionality:

• Large MTU
• Resilient handles

For more information, see Technical Report TR-3740 or the SMB 2.1 protocol specification.
Supported SMB 3.0 functionality

Clustered Data ONTAP 8.2 and later supports the SMB 3.0 protocol on Storage Virtual Machines (SVMs) with FlexVol volumes. SMB 3.0 provides important enhancements, including enhancements that facilitate transparent failover and giveback and other nondisruptive operations.

Support for SMB 3.0 is enabled automatically when you create a CIFS server.

Data ONTAP supports the following SMB 3.0 functionality:

• Continuously available share property
  A new share property that, along with persistent handles, allows SMB clients that are connected to shares that are configured to use the continuously available share property to transparently reconnect to a CIFS server following disruptive events such as failover and giveback operations.

• Persistent handles
  Enables clients to transparently reconnect to disconnected SMB sessions after certain disruptive events. A persistent handle is preserved after a disconnection. Persistent handles block other file opens while waiting for a reconnection. Along with the continuously available share property, persistent handles provide support for certain nondisruptive operations.

• Remote VSS for SMB shares
  Remote VSS (Volume Shadow Copy Service) for SMB provides the functionality that allows VSS-enabled backup services to create application-consistent volume shadow copies of VSS-aware applications that access data stored over SMB 3.0 shares.

• Witness
  Enables a CIFS server providing SMB shares to Hyper-V and SQL application servers to promptly notify the application servers about network failures.

• ODX copy offload
  ODX enables data transfers within or between ODX-enabled storage servers without transferring the data through the Windows client.

• BranchCache version 2
  Provides enhanced functionality, including smaller, variable-sized content segments, which increases the reuse of existing cached content.

• SMB Encryption
  Provides enhanced security for client SMB connections by providing end-to-end encryption of SMB data on the network.

Data ONTAP does not support the following SMB 3.0 functionality:

• SMB Multichannel
• SMB Direct
• SMB Directory Leasing

For more information, see the SMB 3.0 protocol specification.
Related tasks

*Enabling or disabling SMB 3.0* on page 107  
*Monitoring oplock status* on page 111  
*Creating an SMB share on a CIFS server* on page 177  
*Creating Data ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server over SMB* on page 393

### Enabling or disabling SMB 2.x

SMB 2.x is enabled by default for CIFS servers on Storage Virtual Machine (SVM) with FlexVol volumes. This allows clients to connect to the CIFS server using SMB 2.x. You can enable or disable SMB 2.x at any time by using a CIFS server option.

#### About this task

The `-smb2-enabled` option enables SMB 2.0 and SMB 2.1.

#### Steps

1. Set the privilege level to advanced:
   ```bash
   set -privilege advanced
   ```

2. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want SMB 2.x to be...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td><code>vserver cifs options modify -vserver vserver_name -smb2-enabled true</code></td>
</tr>
<tr>
<td>Disabled</td>
<td><code>vserver cifs options modify -vserver vserver_name -smb2-enabled false</code></td>
</tr>
</tbody>
</table>

3. Return to the admin privilege level:
   ```bash
   set -privilege admin
   ```

#### Example

The following example enables SMB 2.x on SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y
cluster1::*> vserver cifs options modify -vserver vs1 -smb2-enabled true
cluster1::*> set -privilege admin
```

#### Related concepts

*Supported SMB 2.0 functionality* on page 103  
*Supported SMB 2.1 functionality* on page 104
Enabling or disabling SMB 3.0

SMB 3.0 is enabled by default for CIFS servers on Storage Virtual Machines (SVMs) with FlexVol volumes. This allows clients that support SMB 3.0 to connect to the CIFS server using SMB 3.0. You can enable or disable SMB 3.0 at any time by using a CIFS server option.

About this task

This option must be enabled if you want to configure continuously available shares.

ODX copy offload requires that SMB 3.0 be enabled. If ODX copy offload is enabled and you disable SMB 3.0, Data ONTAP automatically disables ODX copy offload. Similarly, if you enable ODX copy offload, Data ONTAP will automatically enable SMB 3.0 if it is not already enabled.

Steps

1. Set the privilege level to advanced:
   
   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want SMB 3.0 to be...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>vserver cifs options modify -vserver vserver_name -smb3-enabled true</td>
</tr>
<tr>
<td>Disabled</td>
<td>vserver cifs options modify -vserver vserver_name -smb3-enabled false</td>
</tr>
</tbody>
</table>

3. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Example

The following commands enable SMB 3.0 on SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y
cluster1::*> vserver cifs options modify -vserver vs1 -smb3-enabled true
cluster1::*> set -privilege admin
```

Related concepts

Supported SMB 3.0 functionality on page 105

Improving client performance with traditional and lease oplocks

Traditional oplocks (opportunistic locks) and lease oplocks enable an SMB client in certain file-sharing scenarios to perform client-side caching of read-ahead, write-behind, and lock information. A
client can then read from or write to a file without regularly reminding the server that it needs access to the file in question. This improves performance by reducing network traffic.

Lease oplocks are an enhanced form of oplocks available with the SMB 2.1 protocol and later. Lease oplocks allow a client to obtain and preserve client caching state across multiple SMB opens originating from itself.

Lease oplocks are not supported on Storage Virtual Machines (SVMs) with Infinite Volumes.

**Write cache data-loss considerations when using oplocks**

Under some circumstances, if a process has an exclusive oplock on a file and a second process attempts to open the file, the first process must invalidate cached data and flush writes and locks. The client must then relinquish the oplock and access to the file. If there is a network failure during this flush, cached write data might be lost.

- **Data-loss possibilities**
  Any application that has write-cached data can lose that data under the following set of circumstances:
  
  - The connection is made using SMB 1.0.
  - It has an exclusive oplock on the file.
  - It is told to either break that oplock or close the file.
  - During the process of flushing the write cache, the network or target system generates an error.

- **Error handling and write completion**
  The cache itself does not have any error handling—the applications do. When the application makes a write to the cache, the write is always completed. If the cache, in turn, makes a write to the target system over a network, it must assume that the write is completed because if it does not, the data is lost.

**Enabling or disabling oplocks when creating SMB shares**

Oplocks allow clients to lock files and cache content locally, which can increase performance for file operations. Oplocks are enabled on SMB shares residing on Storage Virtual Machines (SVMs) with FlexVol volumes by default. In some circumstances, you might want to disable oplocks. You can enable or disable oplocks on a share-by-share basis.

**About this task**

If oplocks are enabled on the volume containing a share but the oplock share property for that share is disabled, oplocks are disabled for that share. Disabling oplocks on a share takes precedence over the volume oplock setting. Disabling oplocks on the share disables both opportunistic and lease oplocks.

You can specify other share properties in addition to specifying the oplock share property by using a comma-delimited list. You can also specify other share parameters.

**Step**

1. Perform the applicable action:
Enable oplocks on a share during share creation

Enter the following command:

```
vserver cifs share create -vserver vserver_name -
share-name share_name -path path_to_share -share-
properties [oplocks,...]
```

Note: If you want the share to have only the default share properties, which are oplocks, browsable, and changenotify enabled, you do not have to specify the -share-properties parameter when creating an SMB share. If you want any combination of share properties other than the default, then you must specify the -share-properties parameter with the list of share properties to use for that share.

Disable oplocks on a share during share creation

Enter the following command:

```
vserver cifs share create -vserver vserver_name -
share-name share_name -path path_to_share -share-
properties [other_share_property,...]
```

Note: When disabling oplocks, you must specify a list of share properties when creating the share, but you should not specify the oplocks property.

Related tasks

- Enabling or disabling oplocks on existing SMB shares on page 109
- Monitoring oplock status on page 111
- Creating an SMB share on a CIFS server on page 177

Enabling or disabling oplocks on existing SMB shares

Oplocks are enabled on SMB shares on Storage Virtual Machines (SVMs) with FlexVol volumes by default. Under some circumstances, you might want to disable oplocks; alternatively, if you have previously disabled oplocks on a share, you might want to reenable oplocks.

About this task

If oplocks are enabled on the volume containing a share, but the oplock share property for that share is disabled, oplocks are disabled for that share. Disabling oplocks on a share takes precedence over enabling oplocks on the volume. Disabling oplocks on the share, disables both opportunistic and lease oplocks. You can enable or disable oplocks on existing shares at any time.

Step

1. Perform the applicable action:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable oplocks on a share by modifying an existing share</td>
<td>Enter the following command:</td>
</tr>
<tr>
<td></td>
<td>vserver share properties add -vserver vserver_name -share-name share_name -share-properties oplocks</td>
</tr>
<tr>
<td></td>
<td>Note: You can specify additional share properties to add by using a comma-delimited list. Newly added properties are appended to the existing list of share properties. Any share properties that you have previously specified remain in effect.</td>
</tr>
</tbody>
</table>
If you want to... | Then...
---|---
Disable oplocks on a share by modifying an existing share | Enter the following command:

\[
\texttt{vserver share properties remove -vserver vserver\_name -share-name share\_name -share-properties oplocks}
\]

**Note:** You can specify additional share properties to remove by using a comma-delimited list.

Share properties that you remove are deleted from the existing list of share properties; however, previously configured share properties that you do not remove remain in effect.

### Examples

The following command enables oplocks for the share named “Engineering” on Storage Virtual Machine (SVM, formerly known as Vserver) vs1:

```bash
cluster1::> vserver cifs share properties add -vserver vs1 -share-name Engineering -share-properties oplocks
```

```bash
cluster1::> vserver cifs share properties show
Vserver   Share            Properties
---------- ----------- ----------------- -----------------
vs1        Engineering  oplocks  browsable  changenotify  showsnapshot
```

The following command disables oplocks for the share named “Engineering” on SVM vs1:

```bash
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name Engineering -share-properties oplocks
```

```bash
cluster1::> vserver cifs share properties show
Vserver   Share            Properties
---------- ----------- ----------------- -----------------
vs1        Engineering  browsable  changenotify  showsnapshot
```

### Related tasks

- Enabling or disabling oplocks when creating SMB shares on page 108
- Monitoring oplock status on page 111
- Adding or removing share properties on an existing SMB share on page 183

### Commands for enabling or disabling oplocks on volumes and qtrees

Oplocks allow clients to lock files and cache content locally, which can increase performance for file operations. You need to know the commands for enabling or disabling oplocks on volumes or qtrees. You also must know when you can enable or disable oplocks on volumes and qtrees.

- Oplocks are enabled on volumes by default.
- You cannot disable oplocks when you create a volume.
- You can enable or disable oplocks on existing volumes for SVMs with FlexVol volumes at any time.
- You cannot disable oplocks on volumes for SVMs with Infinite Volume.
• You can enable oplocks on qtrees for SVMs with FlexVol volumes.
  If you do not specify an oplock setting when creating a qtree, the qtree inherits the oplock setting of the parent volume. However, if you do specify an oplock setting on the qtree, it takes precedence over the oplock setting on the volume.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable oplocks on volumes or qtrees</td>
<td><code>volume qtree oplocks</code> with the <code>-oplock-mode</code> parameter set to <code>enable</code></td>
</tr>
<tr>
<td>Disable oplocks on volumes or qtrees</td>
<td><code>volume qtree oplocks</code> with the <code>-oplock-mode</code> parameter set to <code>disable</code></td>
</tr>
</tbody>
</table>

**Related tasks**

*Monitoring oplock status* on page 111

**Monitoring oplock status**

You can monitor and display information about oplock status. You can use this information to determine which files have oplocks, what the oplock level and oplock state level are, and whether oplock leasing is used. You can also determine information about locks that you might need to break manually.

**About this task**

You can display information about all oplocks in summary form or in a detailed list form. You can also use optional parameters to display information about a smaller subset of existing locks. For example, you can specify that the output return only locks with the specified client IP address or with the specified path.

You can display the following information about traditional and lease oplocks:

• SVM, node, volume, and LIF on which the oplock is established

• Lock UUID

• IP address of the client with the oplock

• Path at which the oplock is established

• Lock protocol (SMB) and type (oplock)

• Lock state

A lock can be in one of the following states:

<table>
<thead>
<tr>
<th>Lock state</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>granted</td>
<td>The lock is established.</td>
</tr>
<tr>
<td>revoking</td>
<td>The server is currently coordinating with the client to change the state of the lock.</td>
</tr>
<tr>
<td>revoked</td>
<td>The lock is undergoing revocation to be downgraded or released.</td>
</tr>
<tr>
<td>adjusted</td>
<td>The lock is undergoing revocation to be replaced by a lock equal to or weaker than the current lock.</td>
</tr>
<tr>
<td>subsumed</td>
<td>The lock is one of a set of locks that will replace a lock that is being revoked.</td>
</tr>
<tr>
<td>waiting</td>
<td>The lock is waiting to be granted because it conflicts with another lock.</td>
</tr>
</tbody>
</table>
### Lock state

<table>
<thead>
<tr>
<th>Lock state</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>denied</td>
<td>The lock has been denied.</td>
</tr>
<tr>
<td>timeout</td>
<td>The lock was waiting and has now timed out.</td>
</tr>
<tr>
<td>gone</td>
<td>The lock is about to be released.</td>
</tr>
<tr>
<td>unused</td>
<td>The lock is allocated but has not been processed into any state.</td>
</tr>
</tbody>
</table>

### Oplock level

A lock can have the following oplock levels:

<table>
<thead>
<tr>
<th>Oplock level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>batch</td>
<td>Permits the client to cache all operations on the file.</td>
</tr>
<tr>
<td>exclusive</td>
<td>Permits the client to cache reads and writes on the file.</td>
</tr>
<tr>
<td>read-batch</td>
<td>Permits the client to cache reads and opens on the file.</td>
</tr>
<tr>
<td>level2</td>
<td>Permits the client to cache reads on the file.</td>
</tr>
<tr>
<td>null</td>
<td>Disallows the client from caching any operations on the file.</td>
</tr>
</tbody>
</table>

### Connection state and SMB expiration time

- Open Group ID if a lease oplock is granted

### Step

1. Display oplock status by using the `vserver locks show` command.

### Examples

The following command displays default information about all locks. The oplock on the displayed file is granted with a `read-batch` oplock level:

```bash
cluster1::> vserver locks show
```

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sharelock Mode: read_write-deny_delete</td>
<td>Oplock Level: read-batch</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following example displays more detailed information about the lock on a file with the path `/data2/data2_2/intro.pptx`. A lease oplock is granted on the file with a `batch` oplock level to a client with an IP address of `10.3.1.3`:

**Note:** When displaying detailed information, the command provides separate output for oplock and sharelock information. This example only shows the output from the oplock section.

```bash
cluster1::> vserver lock show -instance -path /data2/data2_2/intro.pptx
```

|-------------|-----------------|-------------------------|-----------------------------|----------------------------------|------------------|----------------|-------------------|-------------------|
Related tasks

- Enabling or disabling oplocks when creating SMB shares on page 108
- Enabling or disabling oplocks on existing SMB shares on page 109

Related references

- Commands for enabling or disabling oplocks on volumes and qtrees on page 110

Applying Group Policy Objects to CIFS servers

Your CIFS server supports Group Policy Objects (GPOs), a set of rules known as *group policy attributes* that apply to computers in an Active Directory environment. You can use GPOs to centrally manage settings for all Storage Virtual Machines (SVMs) on the cluster belonging to the same Active Directory domain.

When GPOs are enabled on your CIFS server, Data ONTAP sends LDAP queries to the Active Directory server requesting GPO information. If there are GPO definitions that are applicable to your CIFS server, the Active Directory server returns the following GPO information:

- GPO name
- Current GPO version
- Location of the GPO definition
- Lists of UUIDs (universally unique identifiers) for GPO policy sets

**Related concepts**

- Securing file access by using Dynamic Access Control (DAC) on page 196
- Auditing NAS events on SVMs with FlexVol volumes on page 421

**Supported GPOs**

Although not all Group Policy Objects (GPOs) are applicable to your CIFS-enabled Storage Virtual Machines (SVMs), SVMs can recognize and process the relevant set of GPOs.

The following GPOs are currently supported on SVMs with FlexVol volumes:

- Advanced audit policy configuration settings:
  - Object access: Central Access Policy staging
  - Specifies the type of events to be audited for central access policy (CAP) staging, including the following settings:
    - Do not audit
Audit only success events

Audit only failure events

Audit both success and failure events

**Note:** If any of the three audit options are set (audit only success events, audit only failure events, audit both success and failure events), clustered Data ONTAP audits both success and failure events.

Set by using the **Audit Central Access Policy Staging** setting in the **Advanced Audit Policy Configuration/Audit Policies/Object Access** GPO.

**Note:** To use advanced audit policy configuration GPO settings, auditing must be configured on the CIFS-enabled SVM to which you want to apply these setting. If auditing is not configured on the SVM, the GPO settings will not be applied and will be dropped.

- Registry settings:
  - Group Policy refresh interval for CIFS-enabled SVM
    Set by using the **Registry** GPO.
  - Group Policy refresh random offset
    Set by using the **Registry** GPO.
  - Hash publication for BranchCache
    The Hash Publication for BranchCache GPO corresponds to the BranchCache operating mode. The following three supported operating modes are supported:
    - Per-share
    - All-shares
    - Disabled
    Set by using the **Registry** GPO.
  - Hash version support for BranchCache
    The following three hash version settings are supported:
    - BranchCache version 1
    - BranchCache version 2
    - BranchCache versions 1 and 2
    Set by using the **Registry** GPO.

**Note:** To use BranchCache GPO settings, BranchCache must be configured on the CIFS-enabled SVM to which you want to apply these setting. If BranchCache is not configured on the SVM, the GPO settings will not be applied and will be dropped.

- Security settings
  - Audit policy and event log
    - Audit logon events
      Specifies the type of logon events to be audited, including the following settings:
      - Do not audit
      - Audit only success events
      - Audit on failure events
• Audit both success and failure events
Set by using the Audit logon events setting in the Local Policies/Audit Policy GPO.

**Note:** If any of the three audit options are set (audit only success events, audit only failure events, audit both success and failure events), clustered Data ONTAP audits both success and failure events.

• Audit object access
Specifies the type of object access to be audited, including the following settings:

  • Do not audit
  • Audit only success events
  • Audit on failure events
  • Audit both success and failure events
Set by using the Audit object access setting in the Local Policies/Audit Policy GPO.

**Note:** If any of the three audit options are set (audit only success events, audit only failure events, audit both success and failure events), clustered Data ONTAP audits both success and failure events.

• Log retention method
Specifies the audit log retention method, including the following settings:

  • Overwrite the event log when size of the log file exceeds the maximum log size
  • Do not overwrite the event log (clear log manually)
Set by using the Retention method for security log setting in the Event Log GPO.

• Maximum log size
Specifies the maximum size of the audit log.
Set by using the Maximum security log size setting in the Event Log GPO.

**Note:** To use audit policy and event log GPO settings, auditing must configured on the CIFS-enabled SVM to which you want to apply these setting. If auditing is not configured on the SVM, the GPO settings will not be applied and will be dropped.

• File system security
Specifies a list of files or directories on which file security is applied through a GPO.
Set by using the File System GPO.

**Note:** The volume path to which the file system security GPO is configured must exist within the SVM.

• Kerberos policy
  • Maximum clock skew
    Specifies maximum tolerance in minutes for computer clock synchronization.
    Set by using the Maximum tolerance for computer clock synchronization setting in the Account Policies/Kerberos Policy GPO.
  • Maximum ticket age
    Specifies maximum lifetime in hours for user ticket.
Set by using the **Maximum lifetime for user ticket** setting in the **Account Policies/Kerberos Policy** GPO.

- **Maximum ticket renew age**
  Specifies maximum lifetime in days for user ticket renewal.
  Set by using the **Maximum lifetime for user ticket renewal** setting in the **Account Policies/Kerberos Policy** GPO.

- **User rights assignment (privilege rights)**
  - **Take ownership**
    Specifies the list of users and groups that have the right to take ownership of any securable object.
    Set by using the **Take ownership of files or other objects** setting in the **Local Policies/User Rights Assignment** GPO.
  - **Security privilege**
    Specifies the list of users and groups that can specify auditing options for object access of individual resources, such as files, folders, and Active Directory objects.
    Set by using the **Manage auditing and security log** setting in the **Local Policies/User Rights Assignment** GPO.
  - **Change notify privilege (bypass traverse checking)**
    Specifies the list of users and groups that can traverse directory trees even though the users and groups might not have permissions on the traversed directory.
    The same privilege is required for users to receive notifications of changes to files and directories. Set by using the **Bypass traverse checking** setting in the **Local Policies/User Rights Assignment** GPO.

- **Registry values**
  - **Signing required setting**
    Specifies whether required SMB signing is enabled or disabled.
    Set by using the **Microsoft network server: Digitally sign communications (always)** setting in the **Security Options** GPO.

- **Restrict anonymous**
  Specifies what the restrictions for anonymous users are and includes the following three GPO settings:
  - **No enumeration of Security Account Manager (SAM) accounts**:
    This security setting determines what additional permissions are granted for anonymous connections to the computer. This option is displayed as **no-enumeration** in Data ONTAP if it is enabled.
    Set by using the **Network access: Do not allow anonymous enumeration of SAM accounts** setting in the **Local Policies/Security Options** GPO.
  - **No enumeration of SAM accounts and shares**
    This security setting determines whether anonymous enumeration of SAM accounts and shares is allowed. This option is displayed as **no-enumeration** in Data ONTAP if it is enabled.
    Set by using the **Network access: Do not allow anonymous enumeration of SAM accounts and shares** setting in the **Local Policies/Security Options** GPO.
  - **Restrict anonymous access to shares and named pipes**
    This security setting restricts anonymous access to shares and pipes. This option is displayed as **no-access** in Data ONTAP if it is enabled.
Set by using the **Network access: Restrict anonymous access to Named Pipes and Shares** setting in the **Local Policies/Security Options** GPO.

When displaying information about defined and applied group policies, the **Resultant restriction for anonymous user** output field provides information about the resultant restriction of the three restrict anonymous GPO settings. The possible resultant restrictions are as follows:

- **no-access**
  The anonymous user is denied access to the specified shares and named pipes, and cannot use enumeration of SAM accounts and shares. This resultant restriction is seen if the **Network access: Restrict anonymous access to Named Pipes and Shares** GPO is enabled.

- **no-enumeration**
  The anonymous user has access to the specified shares and named pipes, but cannot use enumeration of SAM accounts and shares. This resultant restriction is seen if both of the following conditions are met:
  
  - The **Network access: Restrict anonymous access to Named Pipes and Shares** GPO is disabled.
  - Either the **Network access: Do not allow anonymous enumeration of SAM accounts** or the **Network access: Do not allow anonymous enumeration of SAM accounts and shares** GPOs is enabled.

- **no-restriction**
  The anonymous user has full access and can use enumeration. This resultant restriction is seen if both of the following conditions are met:
  
  - The **Network access: Restrict anonymous access to Named Pipes and Shares** GPO is disabled.
  - Both the **Network access: Do not allow anonymous enumeration of SAM accounts** and **Network access: Do not allow anonymous enumeration of SAM accounts and shares** GPOs are disabled.

- **Restricted Groups**
  You can configure restricted groups to centrally manage membership of either built-in or user-defined groups. When you apply a restricted group through a group policy, the membership of a CIFS server local group is automatically set to match the membership-list settings defined in the applied group policy.
  Set by using the **Restricted Groups** GPO.

- **Central access policy settings**
  Specifies a list of central access policies. Central access policies and the associated central access policy rules determine access permissions for multiple files on the SVM.

**Related concepts**

- *Securing file access by using Dynamic Access Control (DAC)* on page 196
- *Auditing NAS events on SVMs with FlexVol volumes* on page 421
- *Kerberos authentication* on page 22
- *Using BranchCache to cache SMB share content at a branch office* on page 336
- *Using SMB signing to enhance network security* on page 85
- *Configuring bypass traverse checking* on page 237
Requirements for using GPOs with your CIFS server

To use Group Policy Objects (GPOs) with your CIFS server, your system must meet several requirements.

- CIFS must be licensed on the cluster.
- A CIFS server must be configured and joined to a Windows Active Directory domain.
- The CIFS server admin status must be on.
- GPOs must be configured and applied to the Windows Active Directory Organizational Unit (OU) containing the CIFS server computer object.
- GPO support must be enabled on the CIFS server.

Enabling or disabling GPO support on a CIFS server

You can enable or disable Group Policy Object (GPO) support on the CIFS server. If you enable GPO support on the CIFS server, applicable GPOs that are defined on the group policy (in this case, the policy applied to the OU containing the CIFS server computer object) are applied to the CIFS server.

Steps

1. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable GPOs</td>
<td>vserver cifs group-policy modify -vserver vserver_name -status enabled</td>
</tr>
<tr>
<td>Disable GPOs</td>
<td>vserver cifs group-policy modify -vserver vserver_name -status disabled</td>
</tr>
</tbody>
</table>

2. Verify that GPO support is in the desired state:

   vserver cifs group-policy show -vserver vserver_name

Example

The following example enables GPO support on Storage Virtual Machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled
cluster1::> vserver cifs group-policy show -vserver vs1

Vserver: vs1
Group Policy Status: enabled
```
How GPOs are updated on the CIFS server

By default, Data ONTAP retrieves and applies Group Policy Object (GPO) changes every 90 minutes. Security settings are refreshed every 16 hours. If you want to update GPOs to apply new GPO policy settings before Data ONTAP automatically updates them, you can trigger a manual update on a CIFS server with a Data ONTAP command.

- By default, all GPOs are verified and updated as needed every 90 minutes. This interval is configurable and can be set using the Refresh interval and Random offset GPO settings.
  Data ONTAP queries Active Directory for changes to GPOs. If the GPO version numbers recorded in Active Directory are higher than those on the CIFS server, Data ONTAP retrieves and applies the new GPOs. If the version numbers are the same, GPOs on the CIFS server are not updated.

- Security Settings GPOs are refreshed every 16 hours. Data ONTAP retrieves and applies Security Settings GPOs every 16 hours, whether or not these GPOs have changed.
  Note: The 16-hour default value cannot be changed in the current Data ONTAP version. It is a Windows client default setting.

- All GPOs can be updated manually with a Data ONTAP command.
  This command simulates the Windows gpupdate.exe /force command.

What to do if GPO updates are failing

Under some circumstances, Group Policy Object (GPO) updates from Windows 2012 domain controllers might fail, which leads to nothing being visible under the Central Access Policy...
Settings section of the output for the `vserver cifs group-policy show-defined` command. You should know how to correct this issue if it occurs.

<table>
<thead>
<tr>
<th>Underlying cause</th>
<th>Remedy</th>
</tr>
</thead>
</table>
| When clustered Data ONTAP attempts to connect to the Windows 2012 domain controller to perform the GPO update, the connection might fail with the error `0xc00000bd (NT STATUS_DUPLICATE_NAME)`. This error occurs when the server name used to make the connection is different from the NetBIOS name of the CIFS server. There are various reasons this might occur, including the use of aliases. Additionally, clustered Data ONTAP pads the NetBIOS name used when connecting to the domain controller to make the name length equal to 15 characters. This can make it appear that the CIFS server name and the NetBIOS name are different. | 1. Disable NetBIOS name checking on the Windows server by adding the following registry key with the value set to 1:
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\DisableStrictNameChecking"
You can learn more about setting this registry key in Microsoft KB article 281308.
Microsoft Support Article 281308: Connecting to SMB share on a Windows 2000-based computer or a Windows Server 2003-based computer may not work with an alias name
2. Reboot the domain controller. |

Manually updating GPO settings on the CIFS server

If you want to update Group Policy Object (GPO) settings on your CIFS server immediately, you can manually update the settings. You can update only changed settings or you can force an update for all settings, including the settings that were applied previously but have not changed.

**Step**

1. Perform the appropriate action:

<table>
<thead>
<tr>
<th>If you want to update...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changed GPO settings</td>
<td><code>vserver cifs group-policy update -vserver vserver_name</code></td>
</tr>
<tr>
<td>All GPO settings</td>
<td><code>vserver cifs group-policy update -vserver vserver_name -force-reapply-all-settings true</code></td>
</tr>
</tbody>
</table>

**Related concepts**

*How GPOs are updated on the CIFS server* on page 119

**Displaying information about GPO configurations**

You can display information about Group Policy Object (GPO) configurations that are defined in Active Directory and about GPO configurations applied to the CIFS server.

**About this task**

You can display information about all GPO configurations defined in the Active Directory of the domain to which the CIFS server belongs, or you can display information only about GPO configurations applied to a CIFS server.
Step

1. Display information about GPO configurations by performing one of the following actions:

<table>
<thead>
<tr>
<th>If you want to display information about all Group Policy configurations...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defined in Active Directory</td>
<td><code>vserver cifs group-policy show-defined -vserver vserver_name</code></td>
</tr>
<tr>
<td>Applied to a CIFS-enabled Storage Virtual Machine (SVM)</td>
<td><code>vserver cifs group-policy show-applied -vserver vserver_name</code></td>
</tr>
</tbody>
</table>

Example

The following example displays the GPO configurations defined in the Active Directory to which the CIFS-enabled SVM with FlexVol volumes named vs1 belongs:

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1
Vserver: vs1
---------------------------------------
GPO Name: Default Domain Policy
  Level: Domain
  Status: enabled
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication Mode for BranchCache: per-share
  Hash Version Support for BranchCache: version1
Security Settings:
  Event Audit and Event Log:
    Audit Logon Events: none
    Audit Object Access: success
    Log Retention Method: overwrite-as-needed
    Max Log Size: 16384
  File Security:
    /vol1/home
    /vol1/dir1
Kerberos:
  Max Clock Skew: 5
  Max Ticket Age: 10
  Max Renew Age: 7
Privilege Rights:
  Take Ownership: usr1, usr2
  Security Privilege: usr1, usr2
  Change Notify: usr1, usr2
Registry Values:
  Signing Required: false
Restrict Anonymous:
  No enumeration of SAM accounts: true
  No enumeration of SAM accounts and shares: false
  Restrict anonymous access to shares and named pipes: true
  Combined restriction for anonymous user: no-access
Restricted Groups:
  gpr1
gpr2
Central Access Policy Settings:
  Policies: cap1
cap2
GPO Name: Resultant Set of Policy
  Status: enabled
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
```
Hash Publication for Mode BranchCache: per-share
Hash Version Support for BranchCache: version1

Security Settings:
Event Audit and Event Log:
  Audit Logon Events: none
  Audit Object Access: success
  Log Retention Method: overwrite-as-needed
  Max Log Size: 16384
File Security:
  /vol1/home
  /vol1/dir1
Kerberos:
  Max Clock Skew: 5
  Max Ticket Age: 10
  Max Renew Age: 7
Privilege Rights:
  Take Ownership: usr1, usr2
  Security Privilege: usr1, usr2
  Change Notify: usr1, usr2
Registry Values:
  Signing Required: false
Restrict Anonymous:
  No enumeration of SAM accounts: true
  No enumeration of SAM accounts and shares: false
  Restrict anonymous access to shares and named pipes: true
  Combined restriction for anonymous user: no-access
Restricted Groups:
gpr1
gpr2

Central Access Policy Settings:
  Policies: cap1
cap2

The following example displays the GPO configurations applied to the CIFS-enabled SVM vs1:

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1
Vserver: vs1
-----------------------------------------------
GPO Name: Default Domain Policy
  Level: Domain
  Status: enabled
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication Mode for BranchCache: per-share
  Hash Version Support for BranchCache: all-versions
Security Settings:
  Event Audit and Event Log:
    Audit Logon Events: none
    Audit Object Access: success
    Log Retention Method: overwrite-as-needed
    Max Log Size: 16384
File Security:
  /vol1/home
  /vol1/dir1
Kerberos:
  Max Clock Skew: 5
  Max Ticket Age: 10
  Max Renew Age: 7
Privilege Rights:
  Take Ownership: usr1, usr2
  Security Privilege: usr1, usr2
  Change Notify: usr1, usr2
Registry Values:
  Signing Required: false
Restrict Anonymous:
  No enumeration of SAM accounts: true
  No enumeration of SAM accounts and shares: false
  Restrict anonymous access to shares and named pipes: true
  Combined restriction for anonymous user: no-access
Restricted Groups:
gpr1
gpr2
```
Central Access Policy Settings:
  Policies: cap1
cap2

GPO Name: Resultant Set of Policy
Level: RSOP
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication Mode for BranchCache: per-share
  Hash Version Support for BranchCache: all-versions
Security Settings:
  Event Audit and Event Log:
    Audit Logon Events: none
    Audit Object Access: success
    Log Retention Method: overwrite-as-needed
    Max Log Size: 16384
  File Security:
    /vol1/home
    /vol1/dir1
  Kerberos:
    Max Clock Skew: 5
    Max Ticket Age: 10
    Max Renew Age: 7
  Privilege Rights:
    Take Ownership: usr1, usr2
    Security Privilege: usr1, usr2
    Change Notify: usr1, usr2
  Registry Values:
    Signing Required: false
  Restrict Anonymous:
    No enumeration of SAM accounts and shares: false
    Restrict anonymous access to shares and named pipes: true
    Combined restriction for anonymous user: no-access
Restricted Groups:
gpr1
gpr2

Related tasks

Enabling or disabling GPO support on a CIFS server on page 118

Displaying detailed information about restricted group GPOs

You can display detailed information about restricted groups that are defined as Group Policy Objects (GPOs) in Active Directory and that are applied to the CIFS server.

About this task

By default, the following information is displayed:

- Group policy name
- Group policy version
- Link

  Specifies the level in which the group policy is configured. Possible output values include the following:

  - **Local** when the group policy is configured in Data ONTAP
  - **Site** when the group policy is configured at the site level in the domain controller
  - **Domain** when the group policy is configured at the domain level in the domain controller
• **OrganizationalUnit** when the group policy is configured at the Organizational Unit (OU) level in the domain controller

• **RSOP** for the resultant set of policies derived from all the group policies defined at various levels

• Restricted group name

• The users and groups who belong to and who do not belong to the restricted group

• The list of groups to which the restricted group is added
  A group can be a member of groups other than the groups listed here.

**Step**

1. Display information about all restricted group GPOs by performing one of the following actions:

<table>
<thead>
<tr>
<th>If you want to display information about all restricted group GPOs...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defined in Active Directory</td>
<td><code>vserver cifs group-policy restricted-group show-defined -vserver vserver_name</code></td>
</tr>
<tr>
<td>Applied to a CIFS server</td>
<td><code>vserver cifs group-policy restricted-group show-applied -vserver vserver_name</code></td>
</tr>
</tbody>
</table>

**Example**

The following example displays information about restricted group GPOs defined in the Active Directory domain to which the CIFS-enabled SVM named vs1 belongs:

```
cluster1::> vserver cifs group-policy restricted-group show-defined -vserver vs1
Vserver: vs1
-------------

  Group Policy Name: gpo1
  Version: 16
     Link: OrganizationalUnit
  Group Name: group1
    Members: user1
    MemberOf: EXAMPLE\group9

  Group Policy Name: Resultant Set of Policy
  Version: 0
     Link: RSOP
  Group Name: group1
    Members: user1
    MemberOf: EXAMPLE\group9
```

The following example displays information about restricted groups GPOs applied to the CIFS-enabled SVM vs1:

```
cluster1::> vserver cifs group-policy restricted-group show-applied -vserver vs1
Vserver: vs1
-------------

  Group Policy Name: gpo1
  Version: 16
     Link: OrganizationalUnit
  Group Name: group1
    Members: user1
    MemberOf: EXAMPLE\group9

  Group Policy Name: Resultant Set of Policy
```
Displaying information about central access policies

You can display detailed information about central access policies that are defined in Active Directory. You can also display information about central access policies that are applied to the CIFS server through GPOs (group policy objects).

About this task

By default, the following information is displayed:

- Vserver name
- Name of the central access policy
- SID
- Description
- Creation time
- Modification time
- Member rules

Step

1. Display information about central access policies by performing one of the following actions:

<table>
<thead>
<tr>
<th>If you want to display information about all central access policies...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defined in Active Directory</td>
<td>vserver cifs group-policy central-access-policy show-defined -vserver vserver_name</td>
</tr>
<tr>
<td>Applied to a CIFS server</td>
<td>vserver cifs group-policy central-access-policy show-applied -vserver vserver_name</td>
</tr>
</tbody>
</table>

Example

The following example displays information for all central access policies defined in Active Directory:

```
cluster1::> vserver cifs group-policy central-access-policy show-defined

Vserver   Name    SID
-------- ---------- -----------------------------------------------
vs1       p1       S-1-17-3386172923-1132908875-3044409393-3993546205
Description: policy #1
Creation Time: Tue Oct 22 09:34:13 2013
Member Rules: r1
vs1       p2       S-1-17-1885229282-1108162114-134354072-822349040
Description: policy #2
```
The following example displays information for all central access policies applied to Storage Virtual Machines (SVMs) on the cluster:

```
cluster1::> vserver cifs group-policy central-access-policy show-applied
Vserver    Name                 SID
-------- -------------------- -----------------------------------------------
vs1      p1                   S-1-17-3386172923-113298875-3044489393-3993546205
         Description: policy #1
         Creation Time: Tue Oct 22 09:34:13 2013
         Member Rules: r1
vs1      p2                   S-1-17-1885229282-1100162114-134354072-822349040
         Description: policy #2
         Creation Time: Tue Oct 22 10:28:20 2013
         Member Rules: r1
         r2
```

Related concepts

*Securing file access by using Dynamic Access Control (DAC)* on page 196

Related tasks

*Displaying information about GPO configurations* on page 120

*Displaying information about central access policy rules* on page 126

Displaying information about central access policy rules

You can display detailed information about central access policy rules that are associated with central access policies defined in Active Directory. You can also display information about central access policies rules that are applied to the CIFS server through central access policy GPOs (group policy objects).

About this task

You can display detailed information about defined and applied central access policy rules. By default, the following information is displayed:

- Vserver name
- Name of the central access rule
- Description
- Creation time
- Modification time
- Current permissions
- Proposed permissions
- Target resources

Step

1. Display information about all central access policy rules by performing one of the following actions:
If you want to display information about all central access policy rules associated with central access policies...

Enter the command...

<table>
<thead>
<tr>
<th>Defined in Active Directory</th>
<th>vserver cifs group-policy central-access-rule show-defined -vserver vserver_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applied to a CIFS server</td>
<td>vserver cifs group-policy central-access-rule show-applied -vserver vserver_name</td>
</tr>
</tbody>
</table>

Example

The following example displays information for all central access policy rules associated with central access policies defined in Active Directory:

```
cluster1::> vserver cifs group-policy central-access-rule show-defined
Vserver   Name
---------- ---------------------
vs1        r1
  Description: rule #1
  Creation Time: Tue Oct 22 09:33:48 2013
  Modification Time: Tue Oct 22 09:33:48 2013

vs1        r2
  Description: rule #2
  Creation Time: Tue Oct 22 10:27:57 2013
  Modification Time: Tue Oct 22 10:27:57 2013
```

The following example displays information for all central access policy rules associated with central access policies applied to Storage Virtual Machines (SVMs) on the cluster:

```
cluster1::> vserver cifs group-policy central-access-rule show-applied
Vserver   Name
---------- ---------------------
vs1        r1
  Description: rule #1
  Creation Time: Tue Oct 22 09:33:48 2013
  Modification Time: Tue Oct 22 09:33:48 2013

vs1        r2
  Description: rule #2
  Creation Time: Tue Oct 22 10:27:57 2013
  Modification Time: Tue Oct 22 10:27:57 2013
```

Related concepts

- *Securing file access by using Dynamic Access Control (DAC)* on page 196

Related tasks

- *Displaying information about GPO configurations* on page 120
- *Displaying information about central access policies* on page 125
Changing CIFS servers computer account passwords

You can change a CIFS server computer account password by manually changing the password or by resetting it. You can also configure a schedule on the CIFS server to update it automatically.

Related tasks

- Configuring CIFS servers for automatic computer account password changes on page 128

Changing or resetting the domain account password

The CIFS server on your Storage Virtual Machine (SVM) has an Active Directory domain account. You can change the password for this account for good security practices, or reset it if the password is lost.

Step

1. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you...</th>
<th>Use the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Know the password and want to change it</td>
<td><code>vserver cifs domain password change</code></td>
</tr>
<tr>
<td>Do not know the password and want to reset it</td>
<td><code>vserver cifs domain password reset</code></td>
</tr>
</tbody>
</table>

See the man page for each command for more information.

Configuring CIFS servers for automatic computer account password changes

For enhanced security, you can configure CIFS servers to automatically schedule Windows Active Directory computer account password changes. By default, the password change schedule is disabled.

Steps

1. Configure a schedule and enable automatic computer account password changes:

   `vserver cifs domain password schedule modify -vserver vserver_name -is-schedule-enabled true -schedule-weekly-interval integer -schedule-randomized-minute integer -schedule-day-of-week cron_dayofweek -schedule-time-of-day HH:MM:SS`

   - `~schedule-weekly-interval` specifies the number of weeks after which the scheduled domain account password change must occur.
   - `~schedule-randomized-minute` specifies the minutes within which the scheduled domain account password change must begin.
   - `~schedule-day-of-week` sets the day of the week when the scheduled domain account password change occurs.
   - `~schedule-time-of-day` sets the time in HH:MM:SS at which the scheduled domain account password change starts.
Example
vserver cifs domain password schedule modify -vserver vs1 -is-schedule-enabled true -schedule-randomized-minute 120 -schedule-weekly-interval 4 -schedule-day-of-week sunday -schedule-time-of-day 23:00:00

2. Verify that the password schedule is configured correctly and is enabled:

Example
vserver cifs domain password schedule show -vserver vserver_name

Vserver: vs1
Is Password Change Schedule Enabled: true
Interval in Weeks for Password Change Schedule: 4
Minutes Within Which Schedule Start Can be Randomized: 120
Last Successful Password Change/Reset Time: -
Schedule Description: Sun@23:00
Warning Message in Case Job Is Deleted: -

Related concepts
Changing CIFS servers computer account passwords on page 128

Related tasks
Disabling automatic computer account password changes on CIFS servers on page 129

Disabling automatic computer account password changes on CIFS servers

If you want to discontinue automatic computer account password changes for your CIFS servers, you can disable the scheduled changes.

Steps

1. Disable automatic computer account password changes by using the vserver cifs domain password schedule modify command.

Example
vserver cifs domain password schedule modify -vserver vs1 -is-schedule-enabled false

2. Verify that the password schedule is disabled by using the vserver cifs domain password schedule show command.

Example
vserver cifs domain password schedule show -vserver vs1

Vserver: vs1
Is Password Change Schedule Enabled: false
Interval in Weeks for Password Change Schedule: 4
Minutes Within Which Schedule Start Can be Randomized: 120
Last Successful Password Change/Reset Time: -
Schedule Description: Sun@23:00
Warning Message in Case Job Is Deleted: -
Managing domain controller connections

You can manage domain controller connections by displaying information about currently discovered LDAP and domain controller servers, resetting and rediscovering LDAP and domain controller servers, managing the preferred domain controller list, and displaying information about currently configured preferred domain controllers.

Displaying information about discovered servers

You can display information related to discovered LDAP servers and domain controllers on your CIFS server.

Step

1. To display information related to discovered servers, enter the following command:
   
   \texttt{vserver cifs domain discovered-servers show}

Example

The following example shows discovered servers for SVM vs1:

\begin{verbatim}
cluster1::> vserver cifs domain discovered-servers show
Node: node1
Vserver: vs1

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Type</th>
<th>Preference</th>
<th>DC-Name</th>
<th>DC-Address</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>example.com</td>
<td>MS-LDAP</td>
<td>adequate</td>
<td>DC-1</td>
<td>1.1.3.4</td>
<td>OK</td>
</tr>
<tr>
<td>example.com</td>
<td>MS-LDAP</td>
<td>adequate</td>
<td>DC-2</td>
<td>1.1.3.5</td>
<td>OK</td>
</tr>
<tr>
<td>example.com</td>
<td>MS-DC</td>
<td>adequate</td>
<td>DC-1</td>
<td>1.1.3.4</td>
<td>OK</td>
</tr>
<tr>
<td>example.com</td>
<td>MS-DC</td>
<td>adequate</td>
<td>DC-2</td>
<td>1.1.3.5</td>
<td>OK</td>
</tr>
</tbody>
</table>
\end{verbatim}

Related tasks

- \textit{Resetting and rediscovering servers} on page 130
- \textit{Stopping or starting the CIFS server} on page 136

Resetting and rediscovering servers

Resetting and rediscovering servers on your CIFS server allows the CIFS server to discard stored information about LDAP servers and domain controllers. After discarding server information, the CIFS server reacquires current information about these external servers. This can be useful when the connected servers are not responding appropriately.

Steps

1. Enter the following command:
   
   \texttt{vserver cifs domain discovered-servers reset-servers -vserver vserver_name}

2. Display information about the newly rediscovered servers:
   
   \texttt{vserver cifs domain discovered-servers show -vserver vserver_name}
Example

The following example resets and rediscovers servers for Storage Virtual Machine (SVM, formerly known as Vserver) vs1:

cluster1::> vserver cifs domain discovered-servers reset-servers -vserver vs1
cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Type</th>
<th>Preference</th>
<th>DC-Name</th>
<th>DC-Address</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>example.com</td>
<td>MS-LDAP</td>
<td>adequate</td>
<td>DC-1</td>
<td>1.1.3.4</td>
<td>OK</td>
</tr>
<tr>
<td>example.com</td>
<td>MS-LDAP</td>
<td>adequate</td>
<td>DC-2</td>
<td>1.1.3.5</td>
<td>OK</td>
</tr>
<tr>
<td>example.com</td>
<td>MS-DC</td>
<td>adequate</td>
<td>DC-1</td>
<td>1.1.3.4</td>
<td>OK</td>
</tr>
<tr>
<td>example.com</td>
<td>MS-DC</td>
<td>adequate</td>
<td>DC-2</td>
<td>1.1.3.5</td>
<td>OK</td>
</tr>
</tbody>
</table>

Related tasks

* Displaying information about discovered servers on page 130
* Stopping or starting the CIFS server on page 136

Adding preferred domain controllers

Data ONTAP automatically discovers domain controllers through DNS. Optionally, you can add one or more domain controllers to the list of preferred domain controllers for a specific domain.

About this task

If a preferred domain controller list already exists for the specified domain, the new list is merged with the existing list.

Step

1. To add to the list of preferred domain controllers, enter the following command:

   ```
   vserver cifs domain preferred-dc add -vserver vserver_name -domain domain_name -preferred-dc IP_address, ...
   ```

   - `vserver vserver_name` specifies the Storage Virtual Machine (SVM) name.
   - `domain domain_name` specifies the fully qualified Active Directory name of the domain to which the specified domain controllers belong.
   - `preferred-dc IP_address,...` specifies one or more IP addresses of the preferred domain controllers, as a comma-delimited list, in order of preference.

Example

The following command adds domain controllers 172.17.102.25 and 172.17.102.24 to the list of preferred domain controllers that the CIFS server on SVM vs1 uses to manage external access to the cifs.lab.example.com domain.

```plaintext
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```
Commands for managing preferred domain controllers

You need to know the commands for adding, displaying, and removing preferred domain controllers.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a preferred domain controller</td>
<td>vserver cifs domain preferred-dc add</td>
</tr>
<tr>
<td>Display preferred domain controllers</td>
<td>vserver cifs domain preferred-dc show</td>
</tr>
<tr>
<td>Remove a preferred domain controller</td>
<td>vserver cifs domain preferred-dc remove</td>
</tr>
</tbody>
</table>

See the man page for each command for more information.

Related tasks

Adding preferred domain controllers on page 131

Managing NetBIOS aliases for CIFS servers

NetBIOS aliases are alternative names for your CIFS server that SMB clients can use when connecting to the CIFS server. Configuring NetBIOS aliases for a CIFS server can be useful when you are consolidating data from other file servers to the CIFS server and want the CIFS server to respond to the original file servers' names.

You can specify a list of NetBIOS aliases when you create the CIFS server or at any time after you create the CIFS server. You can add or remove NetBIOS aliases from the list at any time. You can connect to the CIFS server using any of the names in the NetBIOS alias list.

Related concepts

Setting up the CIFS server on page 50

Related tasks

Displaying information about NetBIOS over TCP connections on page 140

Adding a list of NetBIOS aliases to the CIFS server

If you want SMB clients to connect to the CIFS server by using an alias, you can create a list of NetBIOS aliases, or you can add NetBIOS aliases to an existing list of NetBIOS aliases.

About this task

- The NetBIOS alias name can be 15 up to characters in length.
- You can configure up to 200 NetBIOS aliases on the CIFS server.
- The following characters are not allowed:
  @ # * ( ) = + [ ] ; : " , < > \ ?
Steps

1. Add the NetBIOS aliases:

   ```bash
   vserver cifs add-netbios-aliases -vserver vserver_name -netbios-aliases NetBIOS_alias,...
   ```

   **Example**

   ```bash
   vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases alias_1,alias_2,alias_3
   ```

   • You can specify one or more NetBIOS aliases by using a comma-delimited list.
   • The specified NetBIOS aliases are added to the existing list.
   • A new list of NetBIOS aliases is created if the list is currently empty.

2. Verify that the NetBIOS aliases were added correctly:

   ```bash
   vserver cifs show -vserver vserver_name -display-netbios-aliases
   ```

   **Example**

   ```bash
   vserver cifs show -vserver vs1 -display-netbios-aliases
   ```

   Vserver: vs1
   Server Name: CIFS_SERVER
   NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3

Related tasks

*Removing NetBIOS aliases from the NetBIOS alias list* on page 133

*Displaying the list of NetBIOS aliases on CIFS servers* on page 134

Removing NetBIOS aliases from the NetBIOS alias list

If you do not need specific NetBIOS aliases for a CIFS server, you can remove those NetBIOS aliases from the list. You can also remove all NetBIOS aliases from the list.

About this task

You can remove more than one NetBIOS alias by using a comma-delimited list. You can remove all of the NetBIOS aliases on a CIFS server by specifying - as the value for the `netbios-aliases` parameter.

Steps

1. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want to remove...</th>
<th>Enter...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specific NetBIOS aliases from the list</td>
<td><code>vserver cifs remove-netbios-aliases -vserver vserver_name -netbios-aliases NetBIOS_alias,...</code></td>
</tr>
<tr>
<td>All NetBIOS aliases from the list</td>
<td><code>vserver cifs remove-netbios-aliases -vserver vserver_name -netbios-aliases -</code></td>
</tr>
</tbody>
</table>

   **Example**

   ```bash
   vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases alias_1
   ```
2. Verify that the specified NetBIOS aliases were removed:

   vserver cifs show -vserver vserver_name -display-netbios-aliases

**Example**

vserver cifs show -vserver vs1 -display-netbios-aliases

| Vserver: vs1 | Server Name: CIFS_SERVER | NetBIOS Aliases: ALIAS_2, ALIAS_3 |

**Displaying the list of NetBIOS aliases on CIFS servers**

You can display the list of NetBIOS aliases. This can be useful when you want to determine the list of names over which SMB clients can make connections to the CIFS server.

**Step**

1. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want to display information about...</th>
<th>Enter...</th>
</tr>
</thead>
<tbody>
<tr>
<td>A CIFS server's NetBIOS aliases</td>
<td>vserver cifs show -display-netbios-aliases</td>
</tr>
<tr>
<td>The list of NetBIOS aliases as part of the detailed CIFS server information</td>
<td>vserver cifs show -instance</td>
</tr>
</tbody>
</table>

**Example**

The following example displays information about a CIFS server's NetBIOS aliases:

vserver cifs show -display-netbios-aliases

| Vserver: vs1 | Server Name: CIFS_SERVER | NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3 |

The following example displays the list of NetBIOS aliases as part of the detailed CIFS server information:

vserver cifs show -instance

| Vserver: vs1 | CIFS Server NetBIOS Name: CIFS_SERVER | NetBIOS Domain/Workgroup Name: EXAMPLE | Fully Qualified Domain Name: EXAMPLE.COM | Default Site Used by LIFs Without Site Membership: | Authentication Style: domain | CIFS Server Administrative Status: up | CIFS Server Description: | List of NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3 |

See the man page for the commands for more information.

**Related tasks**

*Adding a list of NetBIOS aliases to the CIFS server* on page 132
Related references

Commands for managing CIFS servers on page 140

Determining whether SMB clients are connected using NetBIOS aliases

You can determine whether SMB clients are connected using NetBIOS aliases, and if so, which NetBIOS alias is used to make the connection. This can be useful when troubleshooting connection issues.

About this task

You must use the `-instance` parameter to display the NetBIOS alias (if any) associated with an SMB connection. If the CIFS server name or an IP address is used to make the SMB connection, the output for the NetBIOS Name field is `-(hyphen)`.

Step

1. Perform the desired action:

<table>
<thead>
<tr>
<th>If you want to display NetBIOS information for...</th>
<th>Enter...</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMB connections</td>
<td><code>vserver cifs sessions show -instance</code></td>
</tr>
<tr>
<td>Connections using a specified NetBIOS alias</td>
<td><code>vserver cifs sessions show -instance -netbios-name netbios_name</code></td>
</tr>
</tbody>
</table>

Example

The following example displays information about the NetBIOS alias used to make the SMB connection with session ID 1:

```
vserver cifs session show -session-id 1 -instance
```

```
Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
Workstation: 10.2.2.50
Authentication Mechanism: NTLMv2
Windows User: EXAMPLE\user1
UNIX User: user1
Open Shares: 2
Open Files: 2
Open Other: 0
Connected Time: 1d 1h 10m 5s
Idle Time: 22s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: ALIAS1
SMB Encryption Status: Unencrypted
```

Managing miscellaneous CIFS server tasks

You can terminate or restart SMB access to CIFS servers, change or reset the domain account password, move the CIFS server to a different OU, change the CIFS server’s domain, display information about NetBIOS over TCP connections, modify or display information about CIFS servers, or delete CIFS servers.

You can also configure the default UNIX user.
Modifying protocols for SVMs

Before you can configure and use NFS or SMB on Storage Virtual Machines (SVMs), you must enable the protocol. This is typically done during SVM setup, but if you did not enable the protocol during setup, you can enable it later by using the `vserver add-protocols` command.

**About this task**

You can also disable protocols on SVMs using the `vserver remove-protocols` command.

**Steps**

1. Check which protocols are currently enabled and disabled for the SVM:

   ```bash
class::> vserver show -vserver vserver_name -protocols
   
   You can also use the `vserver show-protocols` command to view the currently enabled protocols on all SVMs in the cluster.
   ```

2. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable a protocol</td>
<td><code>vserver add-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]</code></td>
</tr>
<tr>
<td>Disable a protocol</td>
<td><code>vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]</code></td>
</tr>
</tbody>
</table>

   See the man page for each command for more information.

3. Confirm that the allowed and disallowed protocols were updated correctly:

   ```bash
class::> vserver show -vserver vserver_name -protocols
   ```

**Example**

The following command displays which protocols are currently enabled and disabled on the SVM named vs1:

```bash
vs1::> vserver show -vserver vs1 -protocols
Vserver       Allowed Protocols         Disallowed Protocols
-----------   ----------------------    -----------------------
vs1           nfs                       cifs, fcp, iscsi, ndmp
```

The following command allows access over SMB by adding `cifs` to the list of enabled protocols on the SVM named vs1:

```bash
vs1::> vserver add-protocols -vserver vs1 -protocols cifs
```

**Related information**

*Clustered Data ONTAP 8.3.1 man page: vserver add-protocols - Add protocols to the Vserver*

*Clustered Data ONTAP 8.3.1 man page: vserver remove-protocols - Remove protocols from the Vserver*

**Stopping or starting the CIFS server**

You can stop the CIFS server on an SVM, which can be useful when performing tasks while users are not accessing data over SMB shares. You can restart SMB access by starting the CIFS server. By
stopping the CIFS server, you can also modify the protocols allowed on the Storage Virtual Machine (SVM).

**About this task**

**Note:** If you stop the CIFS server, established SMB sessions are terminated and their open files are closed. Workstations with cached data will not be able to save those changes, which could result in data loss.

**Steps**

1. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop the CIFS server</td>
<td>`vserver cifs stop -vserver vserver_name [-foreground {true</td>
</tr>
<tr>
<td>Start the CIFS server</td>
<td>`vserver cifs start -vserver vserver_name [-foreground {true</td>
</tr>
</tbody>
</table>

-`-foreground` specifies whether the command should execute in the foreground or background. If you do not enter this parameter, it is set to `true`, and the command is executed in the foreground.

2. Verify that the CIFS server administrative status is correct by using the `vserver cifs show` command.

**Example**

The following commands start the CIFS server on SVM vs1:

```bash
cluster1::> vserver start -vserver vs1
cluster1::> vserver cifs show -vserver vs1
```

```
Vserver: vs1
   CIFS Server NetBIOS Name: VS1
   NetBIOS Domain/Workgroup Name: DOMAIN
   Fully Qualified Domain Name: DOMAIN.LOCAL
   Default Site Used by LIFs Without Site Membership: 
   Authentication Style: domain
   CIFS Server Administrative Status: up
```

**Related tasks**

- *Displaying information about discovered servers* on page 130
- *Resetting and rediscovering servers* on page 130

**Moving CIFS servers to different OUs**

The CIFS server create-process uses the default organizational unit (OU) CN=Computers during setup unless you specify a different OU. You can move CIFS servers to different OUs after setup.

**Steps**

1. On the Windows server, open the **Active Directory Users and Computers** tree.
2. Locate the Active Directory object for the Storage Virtual Machine (SVM).
3. Right-click the object and select **Move**.
4. Select the OU that you want to associate with the SVM

**Result**
The SVM object is placed in the selected OU.

**Related concepts**
- *Setting up the CIFS server* on page 50

**Modifying the dynamic DNS domain on the SVM before moving the CIFS server**

If you want the Active Directory-integrated DNS server to dynamically register the CIFS server's DNS records in DNS when you move the CIFS server to another domain, you must modify dynamic DNS (DDNS) on the Storage Virtual Machine (SVM) before moving the CIFS server.

**Before you begin**
DNS name services must be modified on the SVM to use the a DNS domain that contains the service location records for the new domain that will contain the CIFS server computer account. If you are using secure DDNS, you must use Active Directory-integrated DNS name servers.

**About this task**
Although DDNS (if configured on the SVM) automatically adds the DNS records for data LIFs to the new domain, the DNS records for the original domain are not automatically deleted from the original DNS server. You must delete them manually.

**Steps**

1. **Modifying the domain for DDNS on the SVM:**
   
   ```bash
   vserver services name-service dns dynamic-update modify -vserver vserver_name -is-enabled true -use-secure {true|false} -domain-name FQDN_used_for_DNS_updates
   
   Example
   vserver services name-service dns dynamic-update modify -vserver vs1 -is-enabled true -use-secure true -domain-name example2.com
   ```

2. **Verify that the DDNS configuration is correct:**
   
   ```bash
   vserver services name-service dns dynamic-update show
   
   Example
   vserver services name-service dns dynamic-update show
   
<table>
<thead>
<tr>
<th>Vserver</th>
<th>Is-Enabled</th>
<th>Use-Secure</th>
<th>Domain Name</th>
<th>TTL</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>true</td>
<td>true</td>
<td>example2.com</td>
<td>24h</td>
</tr>
</tbody>
</table>
Joining an SVM to an Active Directory domain

You can join a Storage Virtual Machine (SVM) to an Active Directory domain without deleting the existing CIFS server by modifying the domain using the `vserver cifs modify` command. You can rejoin the current domain or join a new one.

**Before you begin**

- The SVM must already have a DNS configuration.
- Before joining the SVM to a new domain, you should ensure that the DNS configuration for the SVM can serve the target domain. The DNS servers must contain the service location records (SRV) for the domain LDAP and domain controller servers.

**About this task**

- The administrative status of the CIFS server must be set to “down” to proceed with Active Directory domain modification.
- If the command completes successfully, the administrative status is automatically set to “up”.
- When joining a domain, this command might take several minutes to complete.

**Steps**

1. Join the SVM to the CIFS server domain:

   ```
   vserver cifs modify -vserver vserver_name -domain domain_name -status-admin down
   ```

   For more information, see the man page for the `vserver cifs modify` command. If you need to reconfigure DNS for the new domain, see the man page for the `vserver dns modify` command.

2. Verify that the CIFS server is in the desired Active Directory domain:

   ```
   vserver cifs show
   ```

**Example**

In the following example, the CIFS server “CIFSSERVER1” on SVM vs1 joins the example2.com domain:

```
cluster1::> vserver cifs modify -vserver vs1 -domain example2.com -status-admin down
cluster1::> vserver cifs show
```

<table>
<thead>
<tr>
<th>Server</th>
<th>Status</th>
<th>Domain/Workgroup</th>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>CIFSSERVER1</td>
<td>up</td>
<td>EXAMPLE2 domain</td>
</tr>
</tbody>
</table>

**Related concepts**

*Setting up the CIFS server* on page 50
Displaying information about NetBIOS over TCP connections

You can display information about NetBIOS over TCP (NBT) connections. This can be useful when troubleshooting NetBIOS-related issues.

Step

1. Use the `vserver cifs nbtstat` command to display information about NetBIOS over TCP connections.

   Note: NetBIOS name service (NBNS) over IPv6 is not supported.

Example

The following example shows the NetBIOS name service information displayed for “cluster1”:

```
cluster1::> vserver cifs nbtstat
   Vserver: vs1
   Node:    cluster1-01
   Interfaces:
   10.10.10.32
   10.10.10.33
   Servers:
   17.17.1.2  (active  )
   NBT Scope:
   [ ]
   NBT Mode:
   [h]
   NBT Name    NetBIOS Suffix   State   Time Left   Type
   ----------- ---------------  ------- ---------   -----  
   CLUSTER_1   00               wins    57          
   CLUSTER_1   20               wins    57          

Vserver: vs1
Node:    cluster1-02
Interfaces:
10.10.10.35
Servers:
17.17.1.2  (active  )
CLUSTER_1   00               wins    58          
CLUSTER_1   20               wins    58          
4 entries were displayed.
```

Commands for managing CIFS servers

You need to know the commands for creating, displaying, modifying, stopping, starting, and deleting CIFS servers. There are also commands to reset and rediscover servers, change or reset machine account passwords, schedule changes for machine account passwords, and add or remove NetBIOS aliases.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a CIFS server</td>
<td><code>vserver cifs create</code></td>
</tr>
<tr>
<td>Display information about a CIFS server</td>
<td><code>vserver cifs show</code></td>
</tr>
<tr>
<td>Modify a CIFS server</td>
<td><code>vserver cifs modify</code></td>
</tr>
<tr>
<td>Move a CIFS server to another domain</td>
<td><code>vserver cifs modify</code></td>
</tr>
<tr>
<td>Stop a CIFS server</td>
<td><code>vserver cifs stop</code></td>
</tr>
<tr>
<td>Start a CIFS server</td>
<td><code>vserver cifs start</code></td>
</tr>
<tr>
<td>Delete a CIFS server</td>
<td><code>vserver cifs delete</code></td>
</tr>
</tbody>
</table>
If you want to... | Use this command...
---|---
Reset and rediscover servers for the CIFS server | `vserver cifs domain discovered-servers reset-servers`
Change the CIFS server's machine account password | `vserver cifs domain password change`
Reset the CIFS server's machine account password | `vserver cifs domain password reset`
Schedule automatic password changes for the CIFS server's machine account | `vserver cifs domain password schedule modify`
Add NetBIOS aliases for the CIFS server | `vserver cifs add-netbios-aliases`
Remove NetBIOS aliases for the CIFS server | `vserver cifs remove-netbios-aliases`

See the man page for each command for more information.

**Related concepts**

*Setting up the CIFS server* on page 50
*What happens to local users and groups when deleting CIFS servers* on page 215

**Using IPv6 for SMB access and CIFS services**

Starting with Data ONTAP 8.2, SMB clients can access files on your Storage Virtual Machine (SVM) over an IPv6 network and can use IPv6 for CIFS service communications.

After you enable IPv6 on the cluster and properly configure data LIFs, IPv6 works immediately. You do not have configure any settings on the SVM and you do not have to enable any CIFS server options.

**Requirements for using IPv6**

Before you can use IPv6 on your CIFS server, you need to know which versions of Data ONTAP and SMB support it and what the license requirements are.

**Data ONTAP version and license requirements**

- Data ONTAP 8.2 and later supports IPv6.
  
  Commands used to configure CIFS servers, SMB access, and CIFS services and features that support IPv6 can use either IPv4 or IPv6 addresses whenever an IP address is a supported command parameter. Similarly, commands supported with IPv6 that display information about IP addresses display both IPv4 and IPv6 addresses.

- No special license is required for IPv6; however, CIFS must be licensed, and a CIFS server must exist on the Storage Virtual Machine (SVM) to use IPv6 with SMB access and CIFS services.

**SMB protocol version requirements**

- For SVMs with FlexVol volumes, Data ONTAP supports IPv6 on all versions of the SMB protocol.

- For SVMs with Infinite Volume, Data ONTAP supports IPv6 on SMB 1.0. This is because SMB 2.x and SMB 3.0 are not supported on SVMs with Infinite Volume.

  **Note:** NetBIOS name service (NBNS) over IPv6 is not supported.
Support for IPv6 with SMB access and CIFS services

If you want to use IPv6 on your CIFS server, you need to be aware of how Data ONTAP supports IPv6 for SMB access and network communication for CIFS services.

Windows client and server support

Data ONTAP provides support for Windows servers and clients that support IPv6. The following describes Microsoft Windows client and server IPv6 support:

- Windows XP and Windows 2003 support IPv6 for SMB file sharing. These versions provide limited support for IPv6.
  If IPv6 addresses are configured, Windows 7 and Windows Server 2008 and later releases use IPv6 by default for Active Directory services. Both NTLM and Kerberos authentication over IPv6 connections are supported.
  All Windows clients supported by Data ONTAP can connect to SMB shares by using IPv6 addresses.

For the latest information about which Windows clients Data ONTAP supports, see the Interoperability Matrix at mysupport.netapp.com/matrix.

Note: NT domains are not supported for IPv6.

Additional CIFS services support

In addition to IPv6 support for SMB file shares and Active Directory services, Data ONTAP provides IPv6 support for the following:

- Client-side services, including offline folders, roaming profiles, folder redirection, and Previous Versions
- Server-side services, including Dynamic home directories (Home Directory feature), symlinks and Widelinks, BranchCache, ODX copy offload, automatic node referrals, and Previous Versions
- File access management services, including the use of Windows local users and groups for access control and rights management, setting file permissions and audit policies using the CLI, security tracing, file locks management, and monitoring SMB activity
- NAS multiprotocol auditing
- FPolicy
- Continuously available shares, Witness protocol, and Remote VSS (used with Hyper-V over SMB configurations)

Name service and authentication service support

Communication with the following name services are supported with IPv6:

- Domain controllers
- DNS servers
- LDAP servers
- KDC servers
• NIS servers

How CIFS servers use IPv6 to connect to external servers

To create a configuration that meets your requirements, you must be aware of how CIFS servers use IPv6 when making connections to external servers.

• Source address selection
  If an attempt is made to connect to an external server, the source address selected must be of the same type as the destination address. For example, if connecting to an IPv6 address, the Storage Virtual Machine (SVM) hosting the CIFS server must have a data LIF or management LIF that has an IPv6 address to use as the source address. Similarly, if connecting to an IPv4 address, the SVM must have a data LIF or management LIF that has an IPv4 address to use as the source address.

• For servers dynamically discovered using DNS, server discovery is performed as follows:
  ◦ If IPv6 is disabled on the cluster, only IPv4 servers addresses are discovered.
  ◦ If IPv6 is enabled on the cluster, both IPv4 and IPv6 server addresses are discovered. Either type might be used depending upon the suitability of the server to which the address belongs and the availability of IPv6 or IPv4 data or management LIFs.

Dynamic server discovery is used for discovering Domain Controllers and their associated services, such as LSA, NETLOGON, Kerberos, and LDAP.

• DNS server connectivity
  Whether the SVM uses IPv6 when connecting to a DNS server depends on the DNS name services configuration. If DNS services are configured to use IPv6 addresses, connections are made by using IPv6. If desired, the DNS name services configuration can use IPv4 addresses so that connections to DNS servers continue to use IPv4 addresses. Combinations of IPv4 and IPv6 addresses can be specified when configuring DNS name services.

• LDAP server connectivity
  Whether the SVM uses IPv6 when connecting to an LDAP server depends on the LDAP client configuration. If the LDAP client is configured to use IPv6 addresses, connections are made by using IPv6. If desired, the LDAP client configuration can use IPv4 addresses so that connections to LDAP servers continue to use IPv4 addresses. Combinations of IPv4 and IPv6 addresses can be specified when configuring the LDAP client configuration.

  Note: The LDAP client configuration is used when configuring LDAP for UNIX user, group, and netgroup name services.

• NIS server connectivity
  Whether the SVM uses IPv6 when connecting to a NIS server depends on the NIS name services configuration. If NIS services are configured to use IPv6 addresses, connections are made by using IPv6. If desired, the NIS name services configuration can use IPv4 addresses so that connections to NIS servers continue to use IPv4 addresses. Combinations of IPv4 and IPv6 addresses can be specified when configuring NIS name services.

  Note: NIS name services are used for storing and managing UNIX user, group, netgroup, and host name objects.

Related tasks

Enabling IPv6 for SMB (cluster administrators only) on page 144
Monitoring and displaying information about IPv6 SMB sessions on page 144
Enabling IPv6 for SMB (cluster administrators only)

IPv6 networks are not enabled during cluster setup. A cluster administrator must enable IPv6 after cluster setup is complete to use IPv6 for SMB. When the cluster administrator enables IPv6, it is enabled for the entire cluster.

Step

1. Enable IPv6:

   `network options ipv6 modify -enabled true`

   For more information about enabling IPv6 on the cluster and configuring IPv6 LIFs, see the *Clustered Data ONTAP Network Management Guide.*

   IPv6 is enabled. IPv6 data LIFs for SMB access can be configured.

Related tasks

*Monitoring and displaying information about IPv6 SMB sessions* on page 144

How to disable IPv6 for SMB

Even though IPv6 is enabled on the cluster using a network option, you cannot disable IPv6 for SMB by using the same command. Instead, Data ONTAP disables IPv6 when the cluster administrator disables the last IPv6-enabled interface on the cluster. You should communicate with the cluster administrator about management of your IPv6 enabled interfaces.

For more information about disabling IPv6 on the cluster, see the *Clustered Data ONTAP Network Management Guide.*

Monitoring and displaying information about IPv6 SMB sessions

You can monitor and display information about SMB sessions that are connected using IPv6 networks. This information is useful in determining which clients are connecting using IPv6 as well as other useful information about IPv6 SMB sessions.

Step

1. Perform the desired action:

<table>
<thead>
<tr>
<th>If you want to determine whether...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMB sessions to a Storage Virtual Machine (SVM) are connected using IPv6</td>
<td><code>vserver cifs session show -vserver vserver_name -instance</code></td>
</tr>
<tr>
<td>IPv6 is used for SMB sessions through a specified LIF address</td>
<td><code>vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address -instance</code></td>
</tr>
</tbody>
</table>

   *LIF_IP_address* is the data LIF's IPv6 address.
Setting up file access using SMB

You must complete a number of steps to allow clients to access files using SMB on the CIFS-enabled Storage Virtual Machine (SVM).

File and directory naming dependencies in a multiprotocol environment

File and directory naming conventions depend on both the network clients’ operating systems and the file-sharing protocols.

The operating system and the file-sharing protocols determine the following:

• Characters a file name can use
• Case-sensitivity of a file name

Characters a file or directory name can use

If you are accessing a file or directory from clients with different operating systems, you should use characters that are valid in both operating systems.

For example, if you use UNIX to create a file or directory, do not use a colon (:) in the name because the colon is not allowed in MS-DOS file or directory names. Because restrictions on valid characters vary from one operating system to another, see the documentation for your client operating system for more information about prohibited characters.

How clustered Data ONTAP creates file and directory names

Clustered Data ONTAP creates and maintains two names for files or directories in any directory that has access from an SMB client: the original long name and a name in 8.3 format.

For file or directory names that exceed the eight character name or the three character extension limit (for files), clustered Data ONTAP generates an 8.3-format name as follows:

• It truncates the original file or directory name to six characters, if the name exceeds six characters.
• It appends a tilde (~) and a number, one through five, to file or directory names that are no longer unique after being truncated.
• In the case of files, it truncates the file name extension to three characters.

For example, if an NFS client creates a file named specifications.html, the 8.3 format file name created by clustered Data ONTAP is specif~1.htm. If this name already exists, clustered Data ONTAP uses a different number at the end of the file name. For example, if an NFS client then creates another file named specifications_new.html, the 8.3 format of specifications_new.html is specif~2.htm.

Case-sensitivity of file and directory names in a multiprotocol environment

File and directory names are case-sensitive for NFS clients and case-insensitive but case-preserving for CIFS clients. You must understand what the implications are in a multiprotocol environment and
the actions you might need to take when specifying the path while creating SMB shares and when accessing data within the shares.

If an SMB client creates a directory named `testdir`, both SMB and NFS clients display the file name as `testdir`. However, if an SMB user later tries to create a directory name `TESTDIR`, the name is not allowed because, to the SMB client, that name currently exists. If an NFS user later creates a directory named `TESTDIR`, NFS and SMB clients display the directory name differently, as follows:

On NFS clients, you see both directory names as they were created, for example `testdir` and `TESTDIR`, because directory names are case-sensitive.

SMB clients use the 8.3 names to distinguish between the two directories. One directory has the base file name. Additional directories are assigned an 8.3 file name.

- On SMB clients, you see `testdir` and `TESTDI~1`.
- Clustered Data ONTAP creates the `TESTDI~1` directory name to differentiate the two directories. In this case, you must use the 8.3 name when specifying a share path while creating or modifying a share on a Storage Virtual Machine (SVM).

Similarly for files, if an SMB client creates `test.txt`, both SMB and NFS clients display the file name as `test.txt`. However, if an SMB user later tries to create `Test.txt`, the name is not allowed because, to the SMB client, that name currently exists. If an NFS user later creates a file named `Test.txt`, NFS and SMB clients display the file name differently, as follows:

On NFS clients, you see both file names as they were created, `test.txt` and `Text.txt`, because file names are case-sensitive.

SMB clients use the 8.3 names to distinguish between the two files. One file has the base file name. Additional files are assigned an 8.3 file name.

- On SMB clients, you see `test.txt` and `TEST~1.TXT`.
- Clustered Data ONTAP creates the `TEST~1.TXT` file name to differentiate the two files.

### Configuring security styles

You configure security styles on FlexVol volumes and qtrees to determine the type of permissions Data ONTAP uses to control access and what client type can modify these permissions.

For information about the security style of Infinite Volumes, see the *Clustered Data ONTAP Infinite Volumes Management Guide*.

#### Related concepts

- *What the security styles and their effects are* on page 20
- *Where and when to set security styles* on page 21
- *How to decide on what security style to use on SVMs with FlexVol volumes* on page 21
- *How security style inheritance works* on page 21
- *Managing how file security is presented to SMB clients for UNIX security-style data* on page 75
Configuring security styles on SVM root volumes

You configure the Storage Virtual Machine (SVM) root volume security style to determine the type of permissions used for data on the root volume of the SVM.

Steps

1. Use the `vserver create` command with the `-rootvolume-security-style` parameter to define the security style.

   The possible options for the root volume security style are `unix`, `ntfs`, or `mixed`. You cannot use `unified` security style because it only applies to Infinite Volumes.

   For more information about the `vserver create` command, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

2. Display and verify the configuration, including the root volume security style of the SVM you created:

   `vserver show -vserver vserver_name`

Configuring security styles on FlexVol volumes

You configure the FlexVol volume security style to determine the type of permissions used for data on FlexVol volumes of the Storage Virtual Machine (SVM).

Steps

1. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If the FlexVol volume...</th>
<th>Use the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does not yet exist</td>
<td><code>volume create</code> and include the <code>-security-style</code> parameter to specify the security style.</td>
</tr>
<tr>
<td>Already exists</td>
<td><code>volume modify</code> and include the <code>-security-style</code> parameter to specify the security style.</td>
</tr>
</tbody>
</table>

   The possible options for the FlexVol volume security style are `unix`, `ntfs`, or `mixed`. You cannot use `unified` security style because it only applies to Infinite Volumes.

   If you do not specify a security style when creating a FlexVol volume, the volume inherits the security style of the root volume.

   For more information about the `volume create` or `volume modify` commands, see the *Clustered Data ONTAP Logical Storage Management Guide*.

2. To display the configuration, including the security style of the FlexVol volume you created, enter the following command:

   `volume show -volume volume_name -instance`

Configuring security styles on qtrees

You configure the qtree volume security style to determine the type of permissions used for data on qtrees.

Steps

1. Perform one of the following actions:
If the qtree… | Use the command…
---|---
Does not exist yet | `volume qtree create` and include the `--security-style` parameter to specify the security style.
Already exists | `volume qtree modify` and include the `--security-style` parameter to specify the security style.

The possible options for the qtree security style are `unix`, `ntfs`, or `mixed`. You cannot use `unified` security style because it only applies to Infinite Volumes.

If you do not specify a security style when creating a qtree, the default security style is `mixed`.

For more information about the `volume qtree create` or `volume qtree modify` commands, see the *Clustered Data ONTAP Logical Storage Management Guide*.

2. To display the configuration, including the security style of the qtree you created, enter the following command:
   ```
   volume qtree show --qtree qtree_name --instance
   ```

**Creating and managing data volumes in NAS namespaces**

To manage file access in a NAS environment, you must manage data volumes and junction points on your Storage Virtual Machine (SVM) with FlexVol volumes. This includes planning your namespace architecture, creating volumes with or without junction points, mounting or unmounting volumes, and displaying information about data volumes and NFS server or CIFS server namespaces.

**Related concepts**
- *What namespaces in SVMs with FlexVol volumes are* on page 15
- *Volume junction usage rules* on page 15
- *How volume junctions are used in SMB and NFS namespaces* on page 16
- *What the typical NAS namespace architectures are* on page 16

**Related tasks**
- *Configuring character mapping for SMB file name translation on FlexVol volumes* on page 161

**Creating data volumes with specified junction points**

You can specify the junction point when you create a data volume. The resultant volume is automatically mounted at the junction point and is immediately available to configure for NAS access.

**Before you begin**

The aggregate in which you want to create the volume must already exist.

**Steps**

1. Create the volume with a junction point:
   ```
   volume create --vserver vserver_name --volume volume_name --aggregate aggregate_name --size {integer[KB|MB|GB|TB|PB]} --security-style {ntfs|unix|mixed} --junction-path junction_path
   ```

   The junction path must start with the root (/) and can contain both directories and junctioned volumes. The junction path does not need to contain the name of the volume. Junction paths are independent of the volume name.
Specifying a volume security style is optional. If you do not specify a security style, Data ONTAP creates the volume with the same security style that is applied to the root volume of the Storage Virtual Machine (SVM). However, the root volume's security style might not be the security style you want applied to the data volume you create. The recommendation is to specify the security style when you create the volume to minimize difficult-to-troubleshoot file-access issues.

The junction path is case insensitive; /ENG is the same as /eng. If you create a CIFS share, Windows treats the junction path as if it is case sensitive. For example, if the junction is /ENG, the path of a CIFS share must start with /ENG, not /eng.

There are many optional parameters that you can use to customize a data volume. To learn more about them, see the man pages for the `volume create` command.

2. Verify that the volume was created with the desired junction point:

   ```bash
test::> volume show -vserver vs1 -volume volume_name -junction
```

### Example

The following example creates a volume named “home4” located on SVM vs1 that has a junction path /eng/home:

```bash
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1 -size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Volume</th>
<th>Active</th>
<th>Junction Path</th>
<th>Path Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>home4</td>
<td>true</td>
<td>/eng/home</td>
<td>RW_volume</td>
</tr>
</tbody>
</table>

### Creating data volumes without specifying junction points

You can create a data volume without specifying a junction point. The resultant volume is not automatically mounted, and is not available to configure for NAS access. You must mount the volume before you can configure SMB shares or NFS exports for that volume.

**Before you begin**

The aggregate in which you want to create the volume must already exist.

**Steps**

1. Create the volume without a junction point by using the following command:

   ```bash
   volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed}
   ```

   Specifying a volume security style is optional. If you do not specify a security style, Data ONTAP creates the volume with the same security style that is applied to the root volume of the Storage Virtual Machine (SVM). However, the root volume's security style might not be the security style you want applied to the data volume. The recommendation is to specify the security style when you create the volume to minimize difficult-to-troubleshoot file-access issues.

   There are many optional parameters that you can use to customize a data volume. To learn more about them, see the man pages for the `volume create` command.

2. Verify that the volume was created without a junction point:

   ```bash
   volume show -vserver vserver_name -volume volume_name -junction
   ```
Example

The following example creates a volume named “sales” located on SVM vs1 that is not mounted at a junction point:

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3 -size 20GB
[Job 3406] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -junction

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Volume</th>
<th>Active</th>
<th>Junction Path</th>
<th>Path Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>data</td>
<td>true</td>
<td>/data</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>home4</td>
<td>true</td>
<td>/eng/home</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>vs1_root</td>
<td></td>
<td>/</td>
<td>-</td>
</tr>
<tr>
<td>vs1</td>
<td>sales</td>
<td></td>
<td>/sales</td>
<td>RW_volume</td>
</tr>
</tbody>
</table>
```

Mounting or unmounting existing volumes in the NAS namespace

A volume must be mounted on the NAS namespace before you can configure NAS client access to data contained in the Storage Virtual Machine (SVM) volumes. You can mount a volume to a junction point if it is not currently mounted. You can also unmount volumes.

About this task

If you unmount a volume, all data within the junction point, including data in volumes with junction points contained within the unmounted volume’s namespace, are inaccessible to NAS clients. When you unmount a volume, data within the volume is not lost. Additionally, existing volume export policies and SMB shares created on the volume or on directories and junction points within the unmounted volume are retained. If you remount the unmounted volume, NAS clients can access the data contained within the volume using existing export policies and SMB shares.

Steps

1. Perform the desired action:

```
If you want to... Enter the command...

Mount a volume  volume mount -vserver vserver_name -volume volume_name -junction-path junction_path

Unmount a volume  volume unmount -vserver vserver_name -volume volume_name
```

2. Verify that the volume is in the desired mount state:

```
volume show -vserver vserver_name -volume volume_name -junction
```

Examples

The following example mounts a volume named “sales” located on SVM vs1 to the junction point /sales:

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 -junction

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Volume</th>
<th>Active</th>
<th>Junction Path</th>
<th>Path Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>data</td>
<td>true</td>
<td>/data</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>home4</td>
<td>true</td>
<td>/eng/home</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>vs1_root</td>
<td></td>
<td>/vs1_root</td>
<td>-</td>
</tr>
<tr>
<td>vs1</td>
<td>sales</td>
<td>true</td>
<td>/sales</td>
<td>RW_volume</td>
</tr>
</tbody>
</table>
```
The following example unmounts a volume named “data” located on SVM vs1:

```
cluster1::> volume unmount -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -junction
```

Displaying volume mount and junction point information

You can display information about mounted volumes for Storage Virtual Machines (SVMs) and the junction points to which the volumes are mounted. You can also determine which volumes are not mounted to a junction point. You can use this information to understand and manage your SVM namespace.

**Step**

1. Perform the desired action:

<table>
<thead>
<tr>
<th>If you want to display...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary information about mounted and unmounted volumes on the SVM</td>
<td><code>volume show -vserver vserver_name -junction</code></td>
</tr>
<tr>
<td>Detailed information about mounted and unmounted volumes on the SVM</td>
<td><code>volume show -vserver vserver_name -volume volume_name -instance</code></td>
</tr>
</tbody>
</table>
| Specific information about mounted and unmounted volumes on the SVM | a. If necessary, you can display valid fields for the `-fields` parameter by using the following command: `volume show -fields ?`
| | b. Display the desired information by using the `-fields` parameter: `volume show -vserver vserver_name -fields filename,...` |

**Examples**

The following example displays a summary of mounted and unmounted volumes on SVM vs1:

```
cluster1::> volume show -vserver vs1 -junction
```

The following example displays information about specified fields for volumes located on SVM vs2:

```
cluster1::> volume show -vserver vs2 -fields vserver,volume,aggregate,size,state,type,security-style, junction-path, junction-parent, node
```
Securing file access by using Storage-Level Access Guard

In addition to securing access by using native file-level and export and share security, you can configure Storage-Level Access Guard, a third layer of security applied by Data ONTAP at the volume level. Storage-Level Access Guard applies to access from all NAS protocols to the storage object to which it is applied.

Storage-Level Access Guard behavior

- Storage-Level Access Guard applies to all the files or all the directories in a storage object. Because all files or directories in a volume are subject to Storage-Level Access Guard settings, inheritance through propagation is not required.

- You can configure Storage-Level Access Guard to apply to files only, to directories only, or to both files and directories within a volume.
  - File and directory security
    Applies to every directory and file within the storage object. This is the default setting.
  - File security
    Applies to every file within the storage object. Applying this security does not affect access to, or auditing of, directories.
  - Directory security
    Applies to every directory within the storage object. Applying this security does not affect access to, or auditing of, files.

- Storage-Level Access Guard is used to restrict permissions. It will never give extra access permissions.

- If you view the security settings on a file or directory from an NFS or SMB client, you do not see the Storage-Level Access Guard security. It’s applied at the storage object level and stored in the metadata used to determine the effective permissions.

- Storage-level security cannot be revoked from a client, even by a system (Windows or UNIX) administrator. It is designed to be modified by storage administrators only.

- You can apply Storage-Level Access Guard to volumes with NTFS or mixed security style.

- You can apply Storage-Level Access Guard to volumes with UNIX security style as long as the Storage Virtual Machine (SVM) containing the volume has a CIFS server configured.

- When volumes are mounted under a volume junction path and if Storage-Level Access Guard is present on that path, it won’t be propagated to volumes mounted under it.

- The Storage-Level Access Guard security descriptor is replicated with SnapMirror data replication and with Storage Virtual Machine (SVM) replication.

- There is special dispensation for virus scanners. Exceptional access is allowed to these servers to screen files and directories, even if Storage-Level Access Guard denies access to the object.
• FPolicy notifications are not sent if access is denied because of Storage-Level Access Guard.

**Storage-Level Access Guard for NFS access**

Only NTFS access permissions are supported for Storage-Level Access Guard. For Data ONTAP to perform security checks on UNIX users for access to data on volumes where Storage-Level Access Guard is applied, the UNIX user must map to a Windows user on the SVM that owns the volume. Storage-Level Access Guard does not apply to SVMs that are UNIX only SVMs and that do not contain CIFS servers.

**Order of access checks**

Access to a file or directory is determined by the combined effect of the export or share permissions, the Storage-Level Access Guard permissions set on volumes, and the native file permissions applied to files and/or directories. All levels of security are evaluated to determine what the effective permissions a file or directory has. The security access checks are performed in the following order:

1. SMB share or NFS export-level permissions
2. Storage-Level Access Guard
3. NTFS file/folder access control lists (ACLs), NFSv4 ACLs, or UNIX mode bits

For more information about configuring Storage-Level Access Guard, see the *Clustered Data ONTAP File Access Management Guide for CIFS*.

**Related concepts**

- *How Data ONTAP secures file and directory access* on page 24
- *Displaying information about file security and audit policies* on page 240
- *Managing NTFS file security, NTFS audit policies, and Storage-Level Access Guard on SVMs using the CLI* on page 251

**Related tasks**

- *Configuring Storage-Level Access Guard* on page 154
- *Performing security traces* on page 285

**Use cases for using Storage-Level Access Guard**

Storage-Level Access Guard provides additional security at the storage level, which is not visible from a client side; therefore, it cannot be revoked by any of the users or administrators from their desktops. There are certain use cases where the ability to control access at the storage level is beneficial.

Typical use cases for this feature include the following scenarios:

- Intellectual property protection by auditing and controlling all users’ access at the storage level
- Storage for financial services companies, including banking and trading groups
- Government services with separate file storage for individual departments
- Universities protecting all student files

**Workflow to configure Storage-Level Access Guard**

The workflow to configure Storage-Level Access Guard (SLAG) uses the same Data ONTAP CLI commands that you use to configure NTFS file permissions and auditing policies. Instead of
configuring file and directory access on a designated target, you configure SLAG on the designated Storage Virtual Machine (SVM) volume.

**Related tasks**

*Configuring Storage-Level Access Guard* on page 154

**Configuring Storage-Level Access Guard**

There are a number of steps you need to follow to configure Storage-Level Access Guard on a volume or qtree. Storage-Level Access Guard provides a level of access security that is set at the storage level. It provides security that applies to all accesses from all NAS protocols to the storage object to which it has been applied.

**Steps**

1. Create a security descriptor by using the `vserver security file-directory ntfs create` command.

    **Example**

    `vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sd1`
vserver security file-directory ntfs show -vserver vs1

Vserver: vs1
NTFS Security Descriptor Name: sd1

<table>
<thead>
<tr>
<th>Account Name</th>
<th>Access</th>
<th>Access Rights</th>
<th>Apply To</th>
</tr>
</thead>
<tbody>
<tr>
<td>BUILTIN\Administrators</td>
<td>allow</td>
<td>full-control</td>
<td>this-folder, sub-folders, files</td>
</tr>
<tr>
<td>BUILTIN\Users</td>
<td>allow</td>
<td>full-control</td>
<td>this-folder, sub-folders, files</td>
</tr>
<tr>
<td>CREATOR OWNER</td>
<td>allow</td>
<td>full-control</td>
<td>this-folder, sub-folders, files</td>
</tr>
<tr>
<td>NT AUTHORITY\SYSTEM</td>
<td>allow</td>
<td>full-control</td>
<td>this-folder, sub-folders, files</td>
</tr>
</tbody>
</table>

A security descriptor is created with the following four default DACL access control entries (ACEs):

If you do not want to use the default entries when configuring Storage-Level Access Guard, you can remove them prior to creating and adding your own ACEs to the security descriptor.

2. Optional: Remove any of the default DACL ACEs from the security descriptor that you do not want configured with Storage-Level Access Guard security:

a. Remove any unwanted DACL ACEs by using the `vserver security file-directory ntfs dacl remove` command.

Example

In this example, three default DACL ACEs are removed from the security descriptor: BUILTIN\Administrators, BUILTIN\Users, and CREATOR OWNER.

```
vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account builtin\users
vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account builtin\administrators
vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
```

b. Verify that the DACL ACEs you do not want to use for Storage-Level Access Guard security are removed from the security descriptor by using the `vserver security file-directory ntfs dacl show` command.

Example

In this example, the output from the command verifies that three default DACL ACEs have been removed from the security descriptor, leaving only the NT AUTHORITY\SYSTEM default DACL ACE entry:

```
vserver security file-directory ntfs dacl show -vserver vs1
```

Vserver: vs1
NTFS Security Descriptor Name: sd1

<table>
<thead>
<tr>
<th>Account Name</th>
<th>Access Type</th>
<th>Access Rights</th>
<th>Apply To</th>
</tr>
</thead>
<tbody>
<tr>
<td>NT AUTHORITY\SYSTEM</td>
<td>allow</td>
<td>full-control</td>
<td>this-folder, sub-folders, files</td>
</tr>
</tbody>
</table>
3. Add one or more DACL entries to a security descriptor by using the `vserver security file-directory ntfs dacl add` command.

**Example**

In this example, two DACL ACEs are added to the security descriptor:

```bash
vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1 -access-type allow -account example\engineering -rights full-control -apply-to this-folder,sub-folders,files
vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users" -rights read -apply-to this-folder,sub-folders,files
```

4. Optional: Add one or more SACL entries to a security descriptor by using the `vserver security file-directory ntfs sacl add` command.

**Example**

In this example, two SACL ACEs are added to the security descriptor:

```bash
vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1 -access-type failure -account "example\Domain Users" -rights read -apply-to this-folder,sub-folders,files
vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering -rights full-control -apply-to this-folder,sub-folders,files
```

5. Verify that the DACL and SACL ACEs are configured correctly by using the `vserver security file-directory ntfs dacl show` and `vserver security file-directory ntfs sacl show` commands, respectively.

**Example**

In this example, the following command displays information about DACL entries for security descriptor “sd1”:

```bash
vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
NTFS Security Descriptor Name: sd1

<table>
<thead>
<tr>
<th>Account Name</th>
<th>Access Type</th>
<th>Access Rights</th>
<th>Apply To</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXAMPLE\Domain Users</td>
<td>allow</td>
<td>read</td>
<td>this-folder, sub-folders, files</td>
</tr>
<tr>
<td>EXAMPLE\engineering</td>
<td>allow</td>
<td>full-control</td>
<td>this-folder, sub-folders, files</td>
</tr>
<tr>
<td>NT AUTHORITY\SYSTEM</td>
<td>allow</td>
<td>full-control</td>
<td>this-folder, sub-folders, files</td>
</tr>
</tbody>
</table>
```

In this example, the following command displays information about SACL entries for security descriptor “sd1”:

```bash
vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
NTFS Security Descriptor Name: sd1

<table>
<thead>
<tr>
<th>Account Name</th>
<th>Access Type</th>
<th>Access Rights</th>
<th>Apply To</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXAMPLE\Domain Users</td>
<td>failure</td>
<td>read</td>
<td>this-folder, sub-folders, files</td>
</tr>
<tr>
<td>EXAMPLE\engineering</td>
<td>success</td>
<td>full-control</td>
<td>this-folder, sub-folders, files</td>
</tr>
</tbody>
</table>
```
6. Create a security policy by using the `vserver security file-directory policy create` command.

**Example**
The following example creates a policy named “policy1”:

```
vserver security file-directory policy create -vserver vs1 -policy-name policy1
```

7. Verify that the policy is correctly configured by using the `vserver security file-directory policy show` command.

**Example**
```
vserver security file-directory policy show
```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Policy Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>policy1</td>
</tr>
</tbody>
</table>

8. Add a task with an associated security descriptor to the security policy by using the `vserver security file-directory policy-task add` command with the `-access-control` parameter set to `slag`.

Even though a policy can contain more than one Storage-Level Access Guard task, you cannot configure a policy to contain both file-directory and Storage-Level Access Guard tasks. A policy must contain either all Storage-Level Access Guard tasks or all file-directory tasks.

**Example**
In this example, a task is added to the policy named “policy1”, which is assigned to security descriptor “sd1”. It is assigned to the `/datavol1` path with the access control type set to “slag”.

```
vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode propagate -ntfs-sd sd1
```

9. Verify that the task is configured correctly by using the `vserver security file-directory policy task show` command.

**Example**
```
vserver security file-directory policy task show -vserver vs1 -policy-name policy1
```

<table>
<thead>
<tr>
<th>Index</th>
<th>File/Folder</th>
<th>Access Control</th>
<th>Security Type</th>
<th>NTFS Mode</th>
<th>NTFS Security Descriptor Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>/datavol1</td>
<td>slag</td>
<td>ntfs</td>
<td>propagate</td>
<td>sd1</td>
</tr>
</tbody>
</table>

10. Apply the Storage-Level Access Guard security policy by using the `vserver security file-directory policy apply` command.

**Example**
```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

The job to apply the security policy is scheduled.
11. Verify that the applied Storage-Level Access Guard security settings are correct by using the `vserver security file-directory show` command.

**Example**

In this example, the output from the command shows that Storage-Level Access Guard security has been applied to the NTFS volume `/datavol1`. Even though the default DACL allowing Full Control to Everyone remains, Storage-Level Access Guard security restricts (and audits) access to the groups defined in the Storage-Level Access Guard settings.

```
vserver security file-directory show -vserver vs1 -path /datavol1
```

<table>
<thead>
<tr>
<th>Vserver: vs1</th>
<th>File Path: /datavol1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Style: ntfs</td>
<td></td>
</tr>
<tr>
<td>Effective Style: ntfs</td>
<td></td>
</tr>
<tr>
<td>DOS Attributes: 10</td>
<td></td>
</tr>
<tr>
<td>DOS Attributes in Text: ----D----</td>
<td></td>
</tr>
<tr>
<td>Unix User Id: 0</td>
<td></td>
</tr>
<tr>
<td>Unix Group Id: 0</td>
<td></td>
</tr>
<tr>
<td>Unix Mode Bits: 777</td>
<td></td>
</tr>
<tr>
<td>Unix Mode Bits in Text: rwxrwxrwx</td>
<td></td>
</tr>
<tr>
<td>ACLs: NTFS Security Descriptor</td>
<td></td>
</tr>
<tr>
<td>Control:0x8004</td>
<td></td>
</tr>
<tr>
<td>Owner:BUILTIN\Administrators</td>
<td></td>
</tr>
<tr>
<td>Group:BUILTIN\Administrators</td>
<td></td>
</tr>
<tr>
<td>DACL - ACEs</td>
<td></td>
</tr>
<tr>
<td>ALLOW-Everyone-0x1f01ff</td>
<td></td>
</tr>
<tr>
<td>ALLOW-Everyone-0x10000000-OI</td>
<td>CI</td>
</tr>
</tbody>
</table>

Storage-Level Access Guard security

SACL (Applies to Directories):
AUDIT-EXAMPLE\Domain Users-0x120089-FA
AUDIT-EXAMPLE\engineering-0x1f01ff-SA

DACL (Applies to Directories):
ALLOW-EXAMPLE\Domain Users-0x120089
ALLOW-EXAMPLE\engineering-0x1f01ff
ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

SACL (Applies to Files):
AUDIT-EXAMPLE\Domain Users-0x120089-FA
AUDIT-EXAMPLE\engineering-0x1f01ff-SA

DACL (Applies to Files):
ALLOW-EXAMPLE\Domain Users-0x120089
ALLOW-EXAMPLE\engineering-0x1f01ff
ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

**Related concepts**

- Managing NTFS file security, NTFS audit policies, and Storage-Level Access Guard on SVMs using the CLI on page 251
- Workflow to configure Storage-Level Access Guard on page 153

**Related tasks**

- Displaying information about Storage-Level Access Guard on page 158
- Removing Storage-Level Access Guard on page 160

**Related information**

- Clustered Data ONTAP 8.3.1 man page: `vserver security file-directory show - Display file/folder security information`

**Displaying information about Storage-Level Access Guard**

Storage-Level Access Guard is a third layer of security applied on a volume or qtree. Storage-Level Access Guard settings cannot be viewed by using the Windows Properties window. You must use the
Data ONTAP CLI to view information about Storage-Level Access Guard security, which you can use to validate your configuration or to troubleshoot file access issues.

About this task

You must supply the name of the Storage Virtual Machine (SVM) and the path to the volume or qtree whose Storage-Level Access Guard security information you want to display. You can display the output in summary form or as a detailed list.

Step

1. Display Storage-Level Access Guard security settings with the desired level of detail:

<table>
<thead>
<tr>
<th>If you want to display information...</th>
<th>Enter the following command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>In summary form</td>
<td><code>vserver security file-directory show -vserver vserver_name -path path</code></td>
</tr>
<tr>
<td>With expanded detail</td>
<td><code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code></td>
</tr>
</tbody>
</table>

Examples

The following example displays Storage-Level Access Guard security information for the NTFS security-style volume with the path `/datavol1` in SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path /datavol1
Vserver: vs1
File Path: /datavol1
File Inode Number: 77
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
Unix User Id: 0
Unix Group Id: 0
Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
Control:0x8004
Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
DACL - ACEs
ALLOW-Everyone-0x1f01ff
ALLOW-Everyone-0x10000000-OI|CI|IO

Storage-Level Access Guard security
SACL (Applies to Directories):
AUDIT-EXAMPLE\Domain Users-0x120089-FA
AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Directories):
ALLOW-EXAMPLE\Domain Users-0x120089
ALLOW-EXAMPLE\engineering-0x1f01ff
ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
SACL (Applies to Files):
AUDIT-EXAMPLE\Domain Users-0x120089-FA
AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Files):
ALLOW-EXAMPLE\Domain Users-0x120089
ALLOW-EXAMPLE\engineering-0x1f01ff
ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

The following example displays the Storage-Level Access Guard information about the mixed security-style volume at the path `/datavol5` in SVM vs1. The top level of this volume has UNIX effective security. The volume has Storage-Level Access Guard security.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /datavol5
Vserver: vs1
File Path: /datavol5
File Inode Number: 3374
```
Removing Storage-Level Access Guard

You can remove Storage-Level Access Guard on a volume or qtree if you no longer want set access security at the storage level. Removing Storage-Level Access Guard does not modify or remove regular NTFS file and directory security.

**Steps**

1. Verify that the volume or qtree has Storage-Level Access Guard configured by using the `vserver security file-directory show` command.

**Example**

`vserver security file-directory show -vserver vs1 -path /datavol2`

---

Vserver: vs1
File Path: /datavol2
File Inode Number: 99
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
Unix User Id: 0
Unix Group Id: 0
Unix Mode Bits: 777
Unix Mode Bits in Text: rwxr-xr-x

**ACLs:** NTFS Security Descriptor
Control:0xbf14
Owner: BUILTIN\Administrators
Group: BUILTIN\Administrators
SACL - ACEs

AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
DACL - ACEs

ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

Storage-Level Access Guard security
DACL (Applies to Directories):
ALLOW-BUILTIN\Administrators-0x1f01ff
ALLOW-CREATOR OWNER-0x1f01ff
ALLOW-EXAMPLE\Domain Admins-0x1f01ff
ALLOW-EXAMPLE\Domain Users-0x120089
ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
DACL (Applies to Files):
2. Remove Storage-Level Access Guard by using the `vserver security file-directory remove-slag` command.

   **Example**

   ```bash
   vserver security file-directory remove-slag -vserver vs1 -path /datavol2
   ```

3. Verify that Storage-Level Access Guard has been removed from the volume or qtree by using the `vserver security file-directory show` command.

   **Example**

   ```bash
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
Vserver: vs1
File Path: /datavol2
File Inode Number: 99
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
Expanded Dos Attributes: -
Unix User Id: 0
Unix Group Id: 0
Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
       Control:0xbf14
       Owner:BUILTIN\Administrators
       Group:BUILTIN\Administrators
       SACL - ACEs
       AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
       DACL - ACEs
       ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
       ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
``` 

### Configuring character mapping for SMB file name translation on FlexVol volumes

NFS clients can create file names that contain characters that are not valid for SMB clients and certain Windows applications. You can configure character mapping for file name translation on FlexVol volumes to allow SMB clients to access files with NFS names that would otherwise not be valid.

**About this task**

When files created by NFS clients are accessed by SMB clients, Data ONTAP looks at the name of the file. If the name is not a valid SMB file name (for example, if it has an embedded colon “:” character), Data ONTAP returns the 8.3 file name that is maintained for each file. However, this causes problems for applications that encode important information into long file names.

Therefore, if you are sharing a file between clients on different operating systems, you should use characters in the file names that are valid in both operating systems.
However, if you have NFS clients that create file names containing characters that are not valid file names for SMB clients, you can define a map that converts the invalid NFS characters into Unicode characters that both SMB and certain Windows applications accept. For example, this functionality supports the CATIA MCAD and Mathematica applications as well as other applications that have this requirement.

You can configure character mapping on a volume-by-volume basis.

You must keep the following in mind when configuring character mapping on a volume:

- Character mapping is not applied across junction points.
  You must explicitly configure character mapping for each junction volume.

- You must make sure that the Unicode characters that are used to represent invalid or illegal characters are characters that do not normally appear in file names; otherwise, unwanted mappings occur.
  For example, if you try to map a colon (:) to a hyphen (-) but the hyphen (-) was used in the file name correctly, a Windows client trying to access a file named “a-b” would have its request mapped to the NFS name of “a:b” (not the desired outcome).

- After applying character mapping, if the mapping still contains an invalid Windows character, Data ONTAP falls back to Windows 8.3 file names.

- In FPolicy notifications, NAS audit logs, and security trace messages, the mapped file names are shown.

- When a SnapMirror relation of type DP is created, the source volume's character mapping is not replicated on the destination DP volume.

Step

1. Configure character mapping:

   `vserver cifs character-mapping create -vserver vserver_name -volume volume_name -mapping mapping_text, ...

   `The mapping consists of a list of source-target character pairs separated by “:”. The characters are Unicode characters entered using hexadecimal digits. For example: 3C:E03C.

   The first value of each `mapping_text` pair that is separated by a colon is the hexadecimal value of the NFS character you want to translate, and the second value is the Unicode value that SMB uses. The mapping pairs must be unique (a one-to-one mapping should exist).

   • Source mapping
   The following table shows the permissible Unicode character set for source mapping:

<table>
<thead>
<tr>
<th>Unicode character</th>
<th>Printed character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x01-0x19</td>
<td>Not applicable</td>
<td>Non-printing control characters</td>
</tr>
<tr>
<td>0x5C</td>
<td>\</td>
<td>Backslash</td>
</tr>
<tr>
<td>0x3A</td>
<td>:</td>
<td>Colon</td>
</tr>
<tr>
<td>0x2A</td>
<td>*</td>
<td>Asterisk</td>
</tr>
<tr>
<td>0x3F</td>
<td>?</td>
<td>Question mark</td>
</tr>
<tr>
<td>0x22</td>
<td>&quot;</td>
<td>Quotation mark</td>
</tr>
<tr>
<td>0x3C</td>
<td>&lt;</td>
<td>Less than</td>
</tr>
<tr>
<td>0x3E</td>
<td>&gt;</td>
<td>Greater than</td>
</tr>
<tr>
<td>Unicode character</td>
<td>Printed character</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>0x7C</td>
<td></td>
<td>Vertical line</td>
</tr>
<tr>
<td>0xB1</td>
<td>±</td>
<td>Plus-minus sign</td>
</tr>
</tbody>
</table>

- **Target mapping**
  You can specify target characters in the “Private Use Area” of Unicode in the following range: U+E0000...U+F8FF.

```
Example
The following command creates a character mapping for a volume named “data” on Storage Virtual Machine (SVM) vs1:
```

```
class101: vserver cifs character-mapping create -volume data -mapping 3c:e17c,3e:f17d,2a:f745
class101: vserver cifs character-mapping show
```

```
Vserver         Volume Name  Character Mapping
--------------  -----------  ------------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

**Related concepts**

*How namespaces and volume junctions affect SMB access on SVMs with FlexVol volumes* on page 15

*Creating and managing data volumes in NAS namespaces* on page 148

**Commands for managing character mappings for SMB file name translation**

You can manage character mapping by creating, modifying, displaying information about, or deleting file character mappings used for SMB file name translation on FlexVol volumes.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create new file character mappings</td>
<td>vserver cifs character-mapping create</td>
</tr>
<tr>
<td>Display information about file character mappings</td>
<td>vserver cifs character-mapping show</td>
</tr>
<tr>
<td>Modify existing file character mappings</td>
<td>vserver cifs character-mapping modify</td>
</tr>
<tr>
<td>Delete file character mappings</td>
<td>vserver cifs character-mapping delete</td>
</tr>
</tbody>
</table>

For more information, see the man page for each command.

**Related tasks**

*Configuring character mapping for SMB file name translation on FlexVol volumes* on page 161

**Creating name mappings**

Data ONTAP uses name mapping to map Windows identities to UNIX identities when accessing data contained on a Storage Virtual Machine (SVM) using SMB connections. It needs this information to
obtain user credentials and provide proper file access regardless of whether the data is of NTFS
security style, UNIX security style, or unified security style.

Name mapping is usually required due to allow multiprotocol access over SMB and NFS to the same
files, regardless of the effective security style applied to the requested files.

You do not have to configure Windows identity to UNIX identity name mapping if you configure the
default UNIX identity to be used instead.

Related concepts
  How name mapping is used to secure SMB file access on SVMs with FlexVol volumes on page 23
  Configuring multidomain name-mapping searches on page 166
  Multidomain searches for UNIX user to Windows user name mappings on page 166

Related tasks
  Configuring the default UNIX user on page 99

Name mapping conversion rules

A Data ONTAP system keeps a set of conversion rules for each Storage Virtual Machine (SVM). Each rule consists of two pieces: a pattern and a replacement. Conversions start at the beginning of the appropriate list and perform a substitution based on the first matching rule. The pattern is a UNIX-style regular expression. The replacement is a string containing escape sequences representing subexpressions from the pattern, as in the UNIX `sed` program.

It is possible to allow NFS access to volumes with NTFS security style for users in a different
domain from the one that the storage system belongs to, provided that the proper name mapping rule
exists.

If a user matches a rule to map to a user in a different domain, the domain must be trusted. To ensure successful mapping to users in other domains for both SMB and NFS access, there must be a bidirectional trust relationship between the domains.

If a user matches a rule but the user cannot authenticate in the other domain because it is untrusted, the mapping fails.

The SVM automatically discovers all bidirectional trusted domains, which are used for multi-domain user mapping searches. Alternatively, you can configure a list of preferred trusted domains that are used for name mapping searches instead of the list of automatically discovered trusted domains.

Regular expressions are not case-sensitive when mapping from Windows to UNIX. However, they are case-sensitive for Kerberos-to-UNIX and UNIX-to-Windows mappings.

As an example, the following rule converts the Windows user named “jones” in the domain named “ENG” into the UNIX user named “jones”.

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Replacement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENG\jones</td>
<td>jones</td>
</tr>
</tbody>
</table>

Note that the backslash is a special character in regular expressions and must be escaped with another backslash.

The caret (^), underscore (_), and ampersand (&) characters can be used as prefixes for digits in replacement patterns. These characters specify uppercase, lowercase, and initial-case transformations, respectively. For instance:

- If the initial pattern is (.+) and the replacement pattern is \\1, then the string jOe is mapped to jOe (no change).
• If the initial pattern is (.+) and the replacement pattern is \_1, then the string jOe is mapped to joe.
• If the initial pattern is (.+) and the replacement pattern is \^1, then the string jOe is mapped to JOE.
• If the initial pattern is (.+) and the replacement pattern is \&1, then the string jOe is mapped to Joe.

If the character following a backslash-underscore (_), backslash-caret (^), or backslash-ampersand (&) sequence is not a digit, then the character following the backslash is used verbatim.

The following example converts any Windows user in the domain named “ENG” into a UNIX user with the same name in NIS.

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Replacement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENG(.+)</td>
<td>\1</td>
</tr>
</tbody>
</table>

The double backslash (\) matches a single backslash. The parentheses denote a subexpression but do not match any characters themselves. The period matches any single character. The asterisk matches zero or more of the previous expression. In this example, you are matching ENG\ followed by one or more of any character. In the replacement, \1 refers to whatever the first subexpression matched.

Assuming the Windows user ENG\jones, the replacement evaluates to jones; that is, the portion of the name following ENG\.

**Note:** If you are using the CLI, you must delimit all regular expressions with double quotation marks ("). For instance, to enter the regular expression (.+) in the CLI, type "(.+)" at the command prompt. Quotation marks are not required in the Web UI.

For further information about regular expressions, see your UNIX system administration documentation, the online UNIX documentation for sed or regex, or Mastering Regular Expressions, published by O’Reilly and Associates.

**Creating a name mapping**

You can use the `vserver name-mapping create` command to create a name mapping. You use name mappings to enable Windows users to access UNIX security style volumes and the reverse.

**About this task**

For each Storage Virtual Machine (SVM), Data ONTAP supports up to 1,024 name mappings for each direction.

**Step**

1. To create a name mapping, enter the following command:

   ```bash
   vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-unix|unix-win} -position integer -pattern text -replacement text
   ```

   - `vserver vserver_name` specifies the SVM name.
   - `direction {krb-unix|win-unix|unix-win}` specifies the mapping direction.
   - `position integer` specifies the desired position in the priority list of a new mapping.
   - `pattern text` specifies the pattern to be matched, up to 256 characters in length.
   - `replacement text` specifies the replacement pattern, up to 256 characters in length.

   When Windows-to-UNIX mappings are created, any CIFS clients that have open connections to the Data ONTAP system at the time the new mappings are created must log out and log back in to see the new mappings.
Examples

The following command creates a name mapping on the SVM named vs1. The mapping is a mapping from UNIX to Windows at position 1 in the priority list. The mapping maps the UNIX user johnd to the Windows user ENG\John.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win -position 1 -pattern johnd -replacement "ENG\John"
```

The following command creates another name mapping on the SVM named vs1. The mapping is a mapping from Windows to UNIX at position 1 in the priority list. The mapping maps every CIFS user in the domain ENG to users in the NIS domain associated with the SVM.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix -position 1 -pattern "ENG\(.+)" -replacement \1"
```

Commands for managing name mappings

There are specific Data ONTAP commands for managing name mappings.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a name mapping</td>
<td>vserver name-mapping create</td>
</tr>
<tr>
<td>Insert a name mapping at a specific position</td>
<td>vserver name-mapping insert</td>
</tr>
<tr>
<td>Display name mappings</td>
<td>vserver name-mapping show</td>
</tr>
<tr>
<td>Exchange the position of two name mappings</td>
<td>vserver name-mapping swap</td>
</tr>
<tr>
<td>Modify a name mapping</td>
<td>vserver name-mapping modify</td>
</tr>
<tr>
<td>Delete a name mapping</td>
<td>vserver name-mapping delete</td>
</tr>
</tbody>
</table>

See the man page for each command for more information.

Configuring multidomain name-mapping searches

You can configure Storage Virtual Machines (SVMs) to perform multidomain name-mapping searches. This enables Data ONTAP to search every bidirectional trusted domain to find a match when performing UNIX user to Windows user name mapping.

Related concepts

- Name mapping conversion rules on page 164
- Multidomain searches for UNIX user to Windows user name mappings on page 166

Related tasks

- Creating a name mapping on page 165
- Enabling or disabling multidomain name mapping searches on page 168

Multidomain searches for UNIX user to Windows user name mappings

Data ONTAP supports multidomain searches when mapping UNIX users to Windows users. All discovered trusted domains are searched for matches to the replacement pattern until a matching
result is returned. Alternatively, you can configure a list of preferred trusted domains, which is used instead of the discovered trusted domain list and is searched in order until a matching result is returned.

**How domain trusts affect UNIX user to Windows user name mapping searches**

To understand how multidomain user name mapping works, you must understand how domain trusts work with Data ONTAP. Active Directory trust relationships with the CIFS server's home domain can be a bidirectional trust or can be one of two types of unidirectional trusts, either an inbound trust or an outbound trust. The home domain is the domain to which the CIFS server on the Storage Virtual Machine (SVM) belongs.

- **Bidirectional trust**
  - With bidirectional trusts, both domains trust each other. If the CIFS server's home domain has a bidirectional trust with another domain, the home domain can authenticate and authorize a user belonging to the trusted domain and vice versa.
  - UNIX user to Windows user name mapping searches can be performed only on domains with bidirectional trusts between the home domain and the other domain.

- **Outbound trust**
  - With an outbound trust, the home domain trusts the other domain. In this case, the home domain can authenticate and authorize a user belonging to the outbound trusted domain.
  - A domain with an outbound trust with the home domain is not searched when performing UNIX user to Windows user name mapping searches.

- **Inbound trust**
  - With an inbound trust, the other domain trusts the CIFS server's home domain. In this case, the home domain cannot authenticate or authorize a user belonging to the inbound trusted domain.
  - A domain with an inbound trust with the home domain is not searched when performing UNIX user to Windows user name mapping searches.

**How wildcards (*) are used to configure multidomain searches for name mapping**

Multidomain name mapping searches are facilitated by the use of wildcards in the domain section of the Windows user name. The following table illustrates how to use wildcards in the domain part of a name mapping entry to enable multidomain searches:

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Replacement</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td>*\administrator</td>
<td>The UNIX user “root” is mapped to the user named “administrator”. All trusted domains are searched in order until the first matching user named “administrator” is found.</td>
</tr>
</tbody>
</table>
| *       | *\*         | Valid UNIX users are mapped to the corresponding Windows users. All trusted domains are searched in order until the first matching user with that name is found.  

**Note:** The pattern *\* is only valid for name mapping from UNIX to Windows, not the other way around.

**How multidomain name searches are performed**

You can choose one of two methods for determining the list of trusted domains used for multidomain name searches:

- Use the automatically discovered bidirectional trust list compiled by Data ONTAP
  - The advantage to this method is that there is no management overhead and that the list is made of trusted domains that Data ONTAP has determined are valid.
The disadvantage is that you cannot choose the order that the trusted domains are searched.

- Use the preferred trusted domain list that you compile
  - The advantage to this method is that you can configure the list of trusted domains in the order that you want them searched.
  - The disadvantage is that there is more management overhead and that the list might become outdated, with some listed domains not being valid, bidirectionally trusted domains.

If a UNIX user is mapped to a Windows user with a wildcard used for the domain section of the user name, the Windows user is looked up in all the trusted domains as follows:

- If a preferred trusted-domain list is configured, the mapped Windows user is looked up in this search list only, in order.
  The search ends as soon as the Windows user is found. If the same Windows user name exists in two different trusted domains, then the user belonging to the domain listed first in the preferred trusted-domain list is returned. If the Windows user is not found in any domains in the preferred list, an error is returned.
  If you want the home domain to be included in the search, it must be included in the preferred trusted domain list.

- If a preferred list of trusted domains is not configured, then the Windows user is looked up in all the bidirectional trusted domains of the home domain.
  The search ends as soon as the Windows user is found. If the same Windows user name exists in two different trusted domains, the user belonging to the domain listed first in the automatically discovered trusted-domain list is returned. You cannot control the order of the trusted domains in the automatically discovered list. If the Windows user is not found in any of the discovered trusted domains, the user is then looked up in the home domain.

- If there are no bidirectionally trusted domains for the home domain, the user is looked up in the home domain.

If a UNIX user is mapped to a Windows user without a domain section in the user name, the Windows user is looked up in the home domain.

For more information about managing the list of bidirectional trusted domains, see the *Clustered Data ONTAP File Access Management Guide for CIFS*.

**Related concepts**
- *How name mapping is used to secure SMB file access on SVMs with FlexVol volumes* on page 23
- *Creating name mappings* on page 163
- *Name mapping conversion rules* on page 164

**Related tasks**
- *Resetting and rediscovering trusted domains* on page 169
- *Displaying information about discovered trusted domains* on page 170
- *Adding, removing, or replacing trusted domains in preferred trusted domain lists* on page 170
- *Displaying information about the preferred trusted domain list* on page 171

**Enabling or disabling multidomain name mapping searches**

With multidomain name mapping searches, you can use a wild card (*) in the domain portion of a Windows name when configuring UNIX user to Windows user name mapping. Using a wild card (*)
in the domain portion of the name enables Data ONTAP to search all domains that have a
bidirectional trust with the domain that contains the CIFS server’s computer account.

**About this task**

As an alternative to searching all bidirectionally trusted domains, you can configure a list of preferred
trapped domains. When a list of preferred trusted domains is configured, Data ONTAP uses the
preferred trusted domain list instead of the discovered bidirectionally trusted domains to perform
multidomain name mapping searches.

- Multidomain name mapping searches are enabled by default.
- This option is available at the advanced privilege level.

**Steps**

1. Set the privilege level to advanced:
   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want multidomain name mapping searches to be...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum-search-enabled true</td>
</tr>
<tr>
<td>Disabled</td>
<td>vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum-search-enabled false</td>
</tr>
</tbody>
</table>

3. Return to the admin privilege level:
   ```
   set -privilege admin
   ```

**Related references**

*Available CIFS server options* on page 70

**Resetting and rediscovering trusted domains**

You can force the rediscovery of all the trusted domains. This can be useful when the trusted domain
servers are not responding appropriately or the trust relationships have changed. Only domains with a
bidirectional trust with the home domain, which is the domain containing the CIFS server’s computer
account, are discovered.

**Step**

1. Reset and rediscover trusted domains by using the `vserver cifs domain trusts rediscover` command.

   **Example**
   ```
   vserver cifs domain trusts rediscover -vserver vs1
   ```

**Related tasks**

*Displaying information about discovered trusted domains* on page 170
Displaying information about discovered trusted domains

You can display information about the discovered trusted domains for the CIFS server's home domain, which is the domain containing the CIFS server's computer account. This can be useful when you want to know which trusted domains are discovered and how they are ordered within the discovered trusted-domain list.

About this task

Only the domains with bidirectional trusts with the home domain are discovered. Since the home domain's domain controller (DC) returns the list of trusted domains in an order determined by the DC, the order of the domains within the list cannot be predicted. By displaying the list of trusted domains, you can determine the search order for multidomain name mapping searches.

The displayed trusted domain information is grouped by node and Storage Virtual Machine (SVM).

Step

1. Display information about discovered trusted domains by using the `vserver cifs domain trusts show` command.

Example

```bash
vserver cifs domain trusts show -vserver vs1
```

<table>
<thead>
<tr>
<th>Node: node1</th>
<th>Vserver: vs1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home Domain</td>
<td>Trusted Domain</td>
</tr>
<tr>
<td>EXAMPLE.COM</td>
<td>CIFS1.EXAMPLE.COM,</td>
</tr>
<tr>
<td>CIFS2.EXAMPLE.COM</td>
<td>EXAMPLE.COM</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Node: node2</th>
<th>Vserver: vs1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home Domain</td>
<td>Trusted Domain</td>
</tr>
<tr>
<td>EXAMPLE.COM</td>
<td>CIFS1.EXAMPLE.COM,</td>
</tr>
<tr>
<td>CIFS2.EXAMPLE.COM</td>
<td>EXAMPLE.COM</td>
</tr>
</tbody>
</table>

Related tasks

- [Resetting and rediscovering trusted domains](#) on page 169

Adding, removing, or replacing trusted domains in preferred trusted domain lists

You can add or remove trusted domains from the preferred trusted domain list for the CIFS server or you can modify the current list. If you configure a preferred trusted domain list, this list is used instead of the discovered bidirectional trusted domains when performing multidomain name mapping searches.

About this task

- If you are adding trusted domains to an existing list, the new list is merged with the existing list with the new entries placed at the end. The trusted domains are searched in the order they appear in the trusted domain list.
• If you are removing trusted domains from the existing list and do not specify a list, the entire trusted domain list for the specified Storage Virtual Machine (SVM) is removed.

• If you modify the existing list of trusted domains, the new list overwrites the existing list.

  **Note:** You should enter only bidirectionally trusted domains in the preferred trusted domain list. Even though you can enter outbound or inbound trust domains into the preferred domain list, they are not used when performing multidomain name mapping searches. Data ONTAP skips the entry for the unidirectional domain and moves on to the next bidirectional trusted domain in the list.

**Step**

1. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want to do the following with the list of preferred trusted domains...</th>
<th>Use the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add trusted domains to the list</td>
<td><code>vserver cifs domain name-mapping-search add -vserver vserver_name -trusted-domains FQDN, ...</code></td>
</tr>
<tr>
<td>Remove trusted domains from the list</td>
<td><code>vserver cifs domain name-mapping-search remove -vserver vserver_name [-trusted-domains FQDN, ...]</code></td>
</tr>
<tr>
<td>Modify the existing list</td>
<td><code>vserver cifs domain name-mapping-search modify -vserver vserver_name -trusted-domains FQDN, ...</code></td>
</tr>
</tbody>
</table>

*`-vserver vserver_name` specifies the SVM name.  
*`-trusted-domain FQDN` specifies a comma-delimited list of fully-qualified domain names of the trusted domains for the home domain. The home domain is the domain which contains the computer account for the CIFS server.*

**Examples**

The following command adds two trusted domains (cifs1.example.com and cifs2.example.com) to the preferred trusted domain list used by SVM vs1:

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1 -trusted-domains cifs1.example.com, cifs2.example.com
```

The following command removes two trusted domains from the list used by SVM vs1:

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1 -trusted-domains cifs1.example.com, cifs2.example.com
```

The following command modifies the trusted domain list used by SVM vs1. The new list replaces the original list:

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1 -trusted-domains cifs3.example.com
```

**Related tasks**

*Displaying information about the preferred trusted domain list* on page 171

**Displaying information about the preferred trusted domain list**

You can display information about which trusted domains are in the preferred trusted domain list and the order in which they are searched if multidomain name mapping searches are enabled. You can
configure a preferred trusted domain list as an alternative to using the automatically discovered trusted domain list.

**Step**

1. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want to display information about the following...</th>
<th>Use the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>All preferred trusted domains in the cluster grouped by Storage Virtual Machine (SVM)</td>
<td>vserver cifs domain name-mapping-search show</td>
</tr>
<tr>
<td>All preferred trusted domains for a specified SVM</td>
<td>vserver cifs domain name-mapping-search show -vserver vserver_name</td>
</tr>
</tbody>
</table>

**Examples**

The following command displays information about all preferred trusted domains on the cluster:

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver         Trusted Domains
--------------  ----------------------------------
vs1             CIFS1.EXAMPLE.COM
```

**Related tasks**

*Adding, removing, or replacing trusted domains in preferred trusted domain lists* on page 170

**Creating and configuring SMB shares**

Before users and applications can access data on the CIFS server over SMB, you must create and configure SMB shares, which is a named access point in a volume. You can customize shares by specifying share parameters and share properties. You can modify an existing share at any time.

When you create an SMB share, Data ONTAP creates a default ACL for the share with Full Control permissions for Everyone.

SMB shares are tied to the CIFS server on the Storage Virtual Machine (SVM). SMB shares are deleted if either the SVM is deleted or the CIFS server with which it is associated is deleted from the SVM. If you re-create the CIFS server on the SVM, you must re-create the SMB shares.

**Related concepts**

*How Data ONTAP secures file and directory access* on page 24

*Managing file access using SMB* on page 212

*Configuring Data ONTAP for Microsoft Hyper-V and SQL Server over SMB solutions* on page 373

**Related tasks**

*Configuring character mapping for SMB file name translation on FlexVol volumes* on page 161
What the default administrative shares are

When you create a CIFS server on your Storage Virtual Machine (SVM), three default administrative shares are automatically created. You should understand what those default shares are and how they are used.

Data ONTAP creates the following default administrative shares when you create the CIFS server:

• ipc$
• admin$
• c$

Because shares that end with the $ character are hidden shares, the default administrative shares are not visible from My Computer, but you can view them by using Shared Folders.

How the ipc$ and admin$ default shares are used

The ipc$ and admin$ shares are used by Data ONTAP and cannot be used by Windows administrators to access data residing on the SVM.

• ipc$ share
  The ipc$ share is a resource that shares the named pipes that are essential for communication between programs. The ipc$ share is used during remote administration of a computer and when viewing a computer's shared resources. You cannot change the share settings, share properties, or ACLs of the ipc$ share. You also cannot rename or delete the ipc$ share.

• admin$ share
  The admin$ share is used during remote administration of the SVM. The path of this resource is always the path to the SVM root. You cannot change the share settings, share properties, or ACLs for the admin$ share. You also cannot rename or delete the admin$ share.

How the c$ default share is used

The c$ share is an administrative share that the cluster or SVM administrator can use to access and manage the SVM root volume.

The following are characteristics of the c$ share:

• The path for this share is always the path to the SVM root volume and cannot be modified.

• The default ACL for the c$ share is Administrator / Full Control.
  This user is the BUILTIN\administrator. By default, the BUILTIN\administrator can map to the share and view, create, modify, or delete files and folders in the mapped root directory. Caution should be exercised when managing files and folders in this directory.

• You can change the c$ share’s ACL.

• You can change the c$ share settings and share properties.

• You cannot delete the c$ share.

• Data ONTAP 8.2.1 and later releases in the 8.2 release family support c$ as a default administrative share that is automatically created during SVM creation.

• If you are upgrading from a version of Data ONTAP that does not support automatic creation of the c$ administrative share and a CIFS server already exists on the SVM, the c$ share is not automatically created upon upgrade.
  In this case, the administrator must manually create the c$ share.
• If you revert or downgrade to a version of Data ONTAP that does not support the c$ share and a
CIFS server already exists on the SVM, the c$ administrative share is not automatically deleted.
The c$ administrative share continues to exist and can be used to administer and manage files and
folders in the SVM root volume.

• The SVM administrator can access the rest of the SVM namespace from the mapped c$ share by
crossing the namespace junctions.

• The c$ share can be accessed by using the Microsoft Management Console.

Related tasks
   Configuring standard NTFS file permissions by using the Windows Security tab on page 190
   Configuring advanced NTFS file permissions using the Windows Security tab on page 192

Share naming considerations

You should keep Data ONTAP share naming considerations in mind when creating SMB shares on
your CIFS server.

Share naming conventions for Data ONTAP are the same as for Windows and include the following
requirements:

• The name of each share must be unique for the CIFS server.

• Share names are not case-sensitive.

• The maximum share name length is 80 characters.

• Unicode share names are supported.

• Share names ending with the $ character are hidden shares.

• The ADMIN$, IPC$, and c$ administrative shares are automatically created on every CIFS server
and are reserved share names.

• You cannot use the share name ONTAP_ADMIN$ when creating a share.

• Share names containing spaces are supported:
  ◦ You cannot use a space as the first character or as the last character in a share name.
  ◦ You must enclose share names containing a space in quotation marks.

   Note: Single quotation marks are considered part of the share name and cannot be used in
   place of quotation marks.

• The following special characters are supported when you name SMB shares:
  ! @ # $ % & ’ _ - . ~ ( ) { }

• The following special characters are not supported when you name SMB shares:
  + [ ] " / : ; | < > , ? * =

Related concepts
   Information you need when creating SMB shares on page 176

Related tasks
   Creating an SMB share on a CIFS server on page 177
Non-Unicode clients not supported

Clustered Data ONTAP only supports Unicode clients when accessing data using CIFS.

**Note:** Because of a limitation, older Macintosh clients running versions Tiger (Mac OS X 10.4.11) and Leopard (Mac OS X 10.5.8) do not fully support Unicode in SMB requests; therefore, they are not supported with Data ONTAP 8.2 or later. To use Macintosh clients when mounting shares with SMB, they must be upgraded to Snow Leopard (Mac OS X 10.6) or later.

Considerations about directory case-sensitivity when creating shares in a multiprotocol environment

If you create shares in a Storage Virtual Machine (SVM) where the 8.3 naming scheme is used to distinguish between directory names where there are only case differences between the names, you must use the 8.3 name in the share path to ensure that the client connects to the desired directory path.

In the following example, two directories named “testdir” and “TESTDIR” were created on a Linux client. The junction path of the volume containing the directories is /home. The first output is from a Linux client and the second output is from an SMB client.

```
ls -l
drwxrwr-x 2 user1 group1 4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1 4096 Apr 17 11:24 TESTDIR

dir
Directory of Z:
04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDIR~1
```

When you create a share to the second directory, you must use the 8.3 name in the share path. In this example, the share path to the first directory is /home/testdir and the share path to the second directory is /home/TESTDIR~1.

Elimination of execute permission requirements on share paths

For versions of Data ONTAP earlier than 8.1.2, if the root of the name space and any contained path components, including junction points, does not allow execute access for a user accessing a folder through an SMB share, access might be denied. Starting with Data ONTAP 8.1.2 and later releases, this restriction is eliminated.

Data ONTAP supports a unified namespace for NAS. A NAS namespace consists of the root of the Storage Virtual Machine (SVM) namespace and FlexVol volumes that are joined together with junctions that present as a hierarchy of subdirectories below the root. This namespace hierarchy presents to the clients as a single SMB share. In essence, junctions stitch together volumes to create a single large file structure.

SMB clients can access the namespace by mapping to the root of the namespace, thus providing access to all the volumes beneath it through the data LIFs on the SVM. Alternatively, clients can also access contained flexible volumes by mounting or mapping at the volume junction points or by mapping using a path to a directory within the namespace, which provides alternative routes to access data contained within the junctioned volumes.

In versions earlier than Data ONTAP 8.1.2, SMB access issues might occur where the root of the namespace or any component in the path to the folder being accessed has an effective UNIX security style (a UNIX security-style volume or a mixed security-style volume with a UNIX effective security). Access issues can occur because of the requirement that the mapped UNIX user must have
execute permissions on the namespace root and on any path component that is of UNIX security style
(either through the owner, group, or other mode bits or through NFSv4 ACLs). This is a requirement,
irrespective of the share location within the namespace hierarchy. This requirement does not apply if
all volumes including the root of the namespace and all LS mirrors are of NTFS security style.

For example, consider the path `/unix1/dir1/dir2/ntfs1/`, in which `unix1` is a UNIX security-
style volume, `ntfs1` is an NTFS security-style volume, and `dir1` and `dir2` are regular directories.
In versions of Data ONTAP earlier than 8.1.2, a user must have execute permissions on `unix1`,
`dir1`, and `dir2` to map a share that points to the path.

Starting with Data ONTAP 8.1.2 and later, this restriction is eliminated. Execute permissions are not
required for the mapped UNIX user to access data over SMB shares. This is true regardless of
security style for the namespace root, any directory component within the path, or any junctioned
volumes.

Be aware that after upgrading to Data ONTAP 8.1.2 or later from a version of Data ONTAP earlier
than 8.1.2, effective access permissions might change as a result of eliminating this requirement. If
you are using the execute permission requirement as a way to restrict SMB access, you might need to
adjust your share or file permissions to apply the desired access restrictions.

Information you need when creating SMB shares

You should be aware of what information you need before creating SMB shares. There are certain
required parameters that you must supply when you create SMB shares and certain choices about
share parameters and share properties that you must make.

When you create a share, you must provide all of the following information:

- The name of the Storage Virtual Machine (SVM) on which to create the share
- The complete path in a volume to the SMB share, beginning with the junction path to the volume
  The SMB share path is case sensitive.
- The name of the share entered by users when they connect to the share

When you create a share, you can optionally specify a description for the share. The share description
appears in the Comment field when you browse the shares on the network.

You can specify the following optional share parameters:

- Whether support for symlinks and widelinks in the share is allowed
- Whether a custom UNIX umask is configured for new files configured on the share
- Whether a custom UNIX umask is configured for new directories configured on the share
- Whether a custom attribute cache lifetime is configured for the attribute cache
  This share setting is useful only if the attribute cache share property is set.
- Whether to configure offline files, and if so, which offline file setting to specify
- Whether operations trigger virus scans on the share, and if so, which operations trigger the scan
  For more information about configuring an antivirus solution, see the Clustered Data ONTAP
  Antivirus Configuration Guide.
- Whether to limit the maximum number of connections on the new share (at the node level) by
  specifying a maximum connections number
- Whether to specify a “force group” to which all SMB users are assigned when accessing files in
  that share
  This share setting has no effect unless the security style of the volume or qtree containing the
  share is mixed or UNIX.
You can specify the following optional share properties:

- Whether the share is a home directory share
- Whether the share supports opportunistic locks
- Whether the share is browsable
- Whether the share shows Snapshot copies
- Whether the share supports change notification
- Whether metadata caching is enabled for the share
- Whether the share is a continuously available share
- Whether the share allows clients to request BranchCache hashes on the files within the share
- Whether the share supports access-based enumeration
- Whether the share allows clients to cache directory enumeration results (namespace caching)
- Whether to require SMB encryption when accessing shares on the SVM

Related concepts
Share naming considerations on page 174

Related tasks
Creating an SMB share on a CIFS server on page 177

Creating an SMB share on a CIFS server

You must create an SMB share before you can share data on a CIFS server with SMB clients. When you create a share, you can customize the share by configuring optional settings, such as specifying how symlinks are presented to clients. You can also set share properties when creating the share.

Steps
1. If necessary, create the directory path structure for the share.

   You must create the directory path structure specified by the -path option in the vserver cifs share create command before creating your share. The vserver cifs share create command checks the path specified in the -path option during share creation. If the specified path does not exist, the command fails.

   If the UNC path (\servername\sharename\filepath) of the share contains more than 256 characters (excluding the initial “\” in the UNC path), then the Security tab in the Windows Properties box is unavailable. This is a Windows client issue rather than a Data ONTAP issue. To avoid this issue, do not create shares with UNC paths with more than 256 characters.

2. Create an SMB share on a CIFS server associated with the specified Storage Virtual Machine (SVM):

   vserver cifs share create -vserver vserver_name -share-name share_name -path path [-share-properties share_properties,...] [-symlink-properties {enable|hide|read_only},...] [-file-umask octal_integer] [-dir-umask octal_integer] [-comment text] [-attribute-cache-ttl [integerh]| [integerm]| [integers]] [-offline-files {none|manual|documents|programs}] [-vscan-fileop-profile {no-scan|standard|strict|writes-only}] [-max-connections-per-share integer] [-force-group-for-create UNIX_group_name]

   vserver vserver_name specifies the CIFS-enabled SVM on which to create the share.
-share-name share_name specifies the name of the new SMB share.

- If this is a home directory share as specified by the value of homedirectory on the -share-properties parameter, you must include either the %w (Windows user name) or the %u (UNIX user name) dynamic variable in the share name. The share name can additionally contain the %d (domain name) dynamic variable (for example, %d/%w) or a static portion in the share name (for example, home1_%w).

- If the share is used by administrators to connect to other users' home directory (the vserver cifs home-directory modify option -is-home-dirs-access-for-admin-enabled is set to true) or by a user to connect to other users' home directory (the advanced vserver cifs home-directory modify option -is-home-dirs-access-for-public-enabled is set to true), the dynamic share name pattern must be preceded by a tilde (~).

-path path specifies the directory path to the SMB share.

- This path must exist.
- A directory path name can be up to 255 characters long.
- If there is a space in the path name, the entire string must be quoted (for example, "/new volume/mount here").
- If this is a home directory share as specified by value of homedirectory on the -share-properties parameter, you can make the path name dynamic by specifying the %w (Windows user name), %u (UNIX user name), or %d (domain name) variables or any of their combinations as a part of the value of this parameter.

-share-properties share_properties specifies an optional list of properties for the share.

- The default initial properties for all shares on FlexVol volumes are oplocks, changenotify, and browsable.

- It is optional to specify share properties when you create a share. However, if you do specify share properties when you create the share, the defaults are not used. If you use the -share-properties parameter when you create a share, you must specify all the share properties that you want to apply to the share using a comma-delimited list.
- For SVMs with Infinite Volume, the default initial properties are oplocks and browsable.

The list of share properties can include one or more of the following:

- homedirectory
  Specifies that this is a home directory share. The CIFS home directory feature enables you to configure a share that maps to different directories based on the user that connects to it and a set of variables. Instead of having to create separate shares for each user, you can configure a single share with a few home directory parameters to define a user's relationship between an entry point (the share) and their home directory (a directory on the SVM).
  Note: This property cannot be added or removed after share creation.

- oplocks
  Specifies that the share uses opportunistic locks, also known as client-side caching. Oplocks are enabled on shares by default; however, some applications do not work well when oplocks are enabled. In particular, database applications such as Microsoft Access are vulnerable to corruption when oplocks are enabled.
  An advantage of shares is that a single path can be shared multiple times, with each share having different properties. For instance, if a path named /dept/finance contains both a database and other types of files, you can create two shares to it, one with oplocks disabled for safe database access and one with oplocks enabled for client-side caching.
• **browseable**
  Specifies that the share can be browsed by Windows clients.

• **showsnapshot**
  Specifies that Snapshot copies can be viewed and traversed by clients.

• **changenotify**
  Specifies that the share supports Change Notify requests. For shares on SVMs with FlexVol volumes, this is a default initial property.
  For shares on SVMs with Infinite Volume, the `changenotify` property is not set by default, and setting it requires the advanced privilege level. When the `changenotify` property is set for a share on SVMs with Infinite Volume, change notifications are not sent for changes to file attributes and time stamps.

• **attributecache**
  Specifies that file attribute caching on the SMB share is enabled to provide faster access of attributes. The default is to disable attribute caching. This property should be enabled only if there are clients connecting to shares over SMB 1.0. This share property is not applicable if clients are connecting to shares over SMB 2.x or SMB 3.0.

• **continuously-available**
  Specifies that SMB 3.0 and later clients that support it are permitted to open files in a persistent manner. Files opened this way are protected from disruptive events, such as failover and giveback. This option is not supported for SVMs with Infinite Volume.

• **branchcache**
  Specifies that the share allows clients to request BranchCache hashes on the files within this share. This option is effective only if you specify `per-share` as the operating mode in the CIFS BranchCache configuration. This option is not supported for SVMs with Infinite Volume.

• **access-based-enumeration**
  Specifies that Access Based Enumeration is enabled on this share. ABE-filtered shared folders are visible to a user based on that individual user's access rights, preventing the display of folders or other shared resources that the user does not have rights to access.

• **namespace-caching**
  Specifies that the SMB clients connecting to this share can cache the directory enumeration results returned by the CIFS servers, which can provide better performance. By default, SMB 1.0 clients do not cache directory enumeration results. Because SMB 2.0 and SMB 3.0 clients cache directory enumeration results by default, specifying this share property provides performance benefits only to SMB 1.0 client connections.

• **encrypt-data**
  This property specifies that SMB encryption must be used when accessing this share. SMB clients that do not support encryption when accessing SMB data will not be able to access this share.

**-symlink-properties** `share_symlink_property` specifies how UNIX symbolic links (symlinks) are presented to SMB clients. You can specify one of the following values:

• **enabled**
  Specifies that symlinks are enabled for read-write access.

• **read_only**
  Specifies that symlinks are enabled for read-only access. This setting does not apply to widelinks. Widelink access is always read-write.
hide

Specifies that SMB clients are prevented from seeing symlinks.

Note: To disable symlinks, you specify the value as "" or "-".

-file-umask octal_integer specifies the default UNIX umask for new files created on the share. If not specified, the umask defaults to 022.

dir-umask octal_integer specifies the default UNIX umask for new directories created on the share. If not specified, the umask defaults to 000.

Note: Accessing an existing directory or file through multiple SMB shares that have different values for the -file-umask and -dir-umask parameters returns consistent permissions and access rights. For instance, assume you have a share named “share1” that has a file umask of 000 and a share named “share2” that has a file umask of 022, and that these shares overlap (that is, can access the same directories). If you create a file named \server\share1\abc, the umask for that file is 000. If you create a file named \server\share2\123, the umask for that file is 022.

-comment text specifies a text description of the share. The description can be up to 255 characters long. If there is a space in the description, the entire string must be quoted (for example, "This is engineering's share.").

-attribute-cache-ttl time_interval specifies the lifetime for the attribute cache share property. Specifying this option is useful only if you specify attributecache as a value of the -share-properties parameter.

-offline-files specifies the caching behavior of Windows clients when accessing data from the share. The value can be one of the following:

- none
  This disallows Windows clients from caching any files on this share.

- manual
  This allows users on Windows clients to manually select files to be cached.

- documents
  This allows Windows clients to cache user documents that are used by the user for offline access.

- programs
  This allows Windows clients to cache programs that are used by the user for offline access. A user can use those files in an offline mode even if the share is available.

-vscan-filop-profile specifies which operations trigger virus scans. The value can be one of the following:

- no-scan
  Specifies that virus scans are never triggered for this share.

- standard
  Specifies that virus scans are triggered by open, close, and rename operations. This is the default profile.

- strict
  Specifies that virus scans are triggered by open, read, close, and rename operations.

- writes-only
  Specifies that virus scans are triggered only when a file that has been modified is closed.

For information about configuring an antivirus solution, see the Clustered Data ONTAP Antivirus Configuration Guide.
-max-connections-per-share specifies the maximum number of simultaneous connections on a share.

- The limit is on a node-by-node basis, not the SVM or cluster basis.
- The default value is 4294967295, which is the maximum value for this parameter.

**Note:** The maximum number of tree connects allowed in a single session is 4096 and is not configurable.

-force-group-for-create specifies that all files that SMB users create in a specific share belong to the same group, also called the force group. The force group must exist in the UNIX group database (files, NIS, or LDAP). This setting has no effect unless the security style of the volume is UNIX or mixed security style. If this setting is specified, the following becomes true for the share:

- The primary GID of the SMB users who access this share is temporarily changed to the GID of the force group.
- All files in this share that SMB users create belong to the same force group, regardless of the primary GID of the file owner.

### Examples

The following command creates an SMB share named “SHARE1” on Storage Virtual Machine (SVM, formerly known as Vserver) “vs1”. Its directory path is /u/eng. Oplocks and browsability are specified on the share, and the UNIX umask is explicitly set as 022 on files and 000 on directories.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name SHARE1 -path /u/eng -share-properties browsable,oplocks -file-umask 022 -dir-umask 000
```

The following command creates an SMB share named “DOCUMENTS” on the SVM “vs1”. The path to the share is /documents. The share uses opportunistic locks (client-side caching), a notification is generated when a change occurs, and the share allows clients to cache user documents on this share.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name DOCUMENTS -path /documents -share-properties changenotify,oplocks -offline-files documents
```

### Related concepts

- What the default administrative shares are on page 173
- Share naming considerations on page 174
- Information you need when creating SMB shares on page 176
- Configuring bypass traverse checking on page 237
- How to optimize SMB user access with the force-group share setting on page 182
- Securing file access by using SMB share ACLs on page 187
- Securing file access by using file permissions on page 190

### Related tasks

- Configuring character mapping for SMB file name translation on FlexVol volumes on page 161
- Creating an SMB share with the force-group share setting on page 182
- Displaying SMB session information on page 298
Displaying information about open SMB files on page 301
Adding or removing share properties on an existing SMB share on page 183

How to optimize SMB user access with the force-group share setting

When you create a share from the Data ONTAP command line to data with UNIX effective security, you can specify that all files created by SMB users in that share belong to the same group, known as the force-group, which must be a predefined group in the UNIX group database. Using a force-group makes it easier to ensure that files can be accessed by SMB users belonging to various groups.

Specifying a force-group is meaningful only if the share is in a UNIX or mixed qtree. There is no need to set a force-group for shares in an NTFS volume or qtree because access to files in these shares is determined by Windows permissions, not UNIX GIDs.

If a force-group has been specified for a share, the following becomes true of the share:

- SMB users in the force-group who access this share are temporarily changed to the GID of the force-group.
  This GID enables them to access files in this share that are not accessible normally with their primary GID or UID.
- All files in this share created by SMB users belong to the same force-group, regardless of the primary GID of the file owner.

When SMB users try to access a file created by NFS, the SMB users' primary GIDs determine access rights.

The force-group does not affect how NFS users access files in this share. A file created by NFS acquires the GID from the file owner. Determination of access permissions is based on the UID and primary GID of the NFS user who is trying to access the file.

Using a force-group makes it easier to ensure that files can be accessed by SMB users belonging to various groups. For example, if you want to create a share to store the company's web pages and give write access to users in the Engineering and Marketing departments, you can create a share and give write access to a force-group named “webgroup1”. Because of the force-group, all files created by SMB users in this share are owned by the “webgroup1” group. In addition, users are automatically assigned the GID of the “webgroup1” group when accessing the share. As a result, all the users can write to this share without you needing to manage the access rights of the users in the Engineering and Marketing departments.

Related tasks
Creating an SMB share with the force-group share setting on page 182

Creating an SMB share with the force-group share setting

You can create an SMB share with the force-group share setting if you want SMB users that access data on volumes or qtrees with UNIX file security to be regarded by Data ONTAP as belonging to the same UNIX group.

Step

1. Create the SMB share:

```
vserver cifs share create -vserver vserver_name -share-name share_name -path path -force-group-for-create UNIX_group_name
```

- `-share-name share_name` specifies the name of the new SMB share, which can be up to 256 characters long.
- `-path path` specifies the path to the share. Path separators can be backward or forward slashes, although Data ONTAP displays them as forward slashes.
If the UNC path (servername\sharename\filepath) of the share contains more than 256 characters (excluding the initial "\" in the UNC path), then the Security tab in the Windows Properties box is unavailable. This is a Windows client issue rather than a Data ONTAP issue. To avoid this issue, do not create shares with UNC paths with more than 256 characters.

-force-group-for-create UNIX_group_name specifies the name of the UNIX group to use as the force-group.

If you want to remove the force-group after the share is created, you can modify the share at any time and specify an empty string ("") as the value for the -force-group-for-create parameter. If you remove the force-group by modifying the share, all existing connections to this share continue to have the previously set force-group as the primary GID.

Example

The following command creates a “webpages” share that is accessible on the web in the /corp/companyinfo directory in which all files that SMB users create are assigned to the webgroup1 group:

vserver cifs share create -vserver vs1 -share-name webpages -path /corp/companyinfo -force-group-for-create webgroup1

Related concepts

How to optimize SMB user access with the force-group share setting on page 182

Related tasks

Creating an SMB share on a CIFS server on page 177

Adding or removing share properties on an existing SMB share

You can customize an existing SMB share by adding or removing share properties. This can be useful if you want to change the share configuration to meet changing requirements in your environment.

Before you begin

The share whose properties you want to modify must exist.

About this task

You need to keep the following in mind when adding share properties:

- You can add one or more share properties by using a comma-delimited list.
- Any share properties that you have previously specified remain in effect. Newly added properties are appended to the existing list of share properties.
- If you specify a new value for share properties that are already applied to the share, the newly specified value replaces the original value.
- You cannot remove share properties by using the vserver cifs share properties add command.
  You can use the vserver cifs share properties remove command to remove share properties.

You need to keep the following in mind when removing share properties:

- You can remove one or more share properties by using a comma-delimited list.
- Any share properties that you have previously specified but do not remove remain in effect.
The available share properties are as follows:

<table>
<thead>
<tr>
<th>Share properties</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>oplocks</td>
<td>This property specifies that the share uses opportunistic locks, also known as client-side caching.</td>
</tr>
<tr>
<td>browsable</td>
<td>This property allows Windows clients to browse the share.</td>
</tr>
<tr>
<td>showsnapshot</td>
<td>This property specifies that Snapshot copies can be viewed and traversed by clients.</td>
</tr>
<tr>
<td>changenotify</td>
<td>This property specifies that the share supports Change Notify requests. For shares on an SVM with FlexVol volumes, this is a default initial property. For shares on an SVM with Infinite Volume, the changenotify property is not set by default, and setting it requires the advanced privilege level. When the changenotify property is set for a share on an SVM with Infinite Volume, change notifications are not sent for changes to file attributes and time stamps.</td>
</tr>
<tr>
<td>attributecache</td>
<td>This property enables the file attribute caching on the SMB share to provide faster access of attributes. The default is to disable attribute caching. This property should be enabled only if there are clients connecting to shares over SMB 1.0. This share property is not applicable if clients are connecting to shares over SMB 2.x or SMB 3.0.</td>
</tr>
<tr>
<td>continuously-available</td>
<td>This property permits SMB clients that support it to open files in a persistent manner. Files opened this way are protected from disruptive events, such as failover and giveback.</td>
</tr>
<tr>
<td>branchcache</td>
<td>This property specifies that the share allows clients to request BranchCache hashes on the files within this share. This option is useful only if you specify “per-share” as the operating mode in the CIFS BranchCache configuration.</td>
</tr>
<tr>
<td>access-based-enumeration</td>
<td>This property specifies that Access Based Enumeration (ABE) is enabled on this share. ABE-filtered shared folders are visible to a user based on that individual user's access rights, preventing the display of folders or other shared resources that the user does not have rights to access.</td>
</tr>
<tr>
<td>namespace-caching</td>
<td>This property specifies that the SMB clients connecting to this share can cache the directory enumeration results returned by the CIFS servers, which can provide better performance. By default, SMB 1 clients do not cache directory enumeration results. Because SMB 2 and SMB 3 clients cache directory enumeration results by default, specifying this share property provides performance benefits only to SMB 1 client connections.</td>
</tr>
<tr>
<td>encrypt-data</td>
<td>This property specifies that SMB encryption must be used when accessing this share. SMB clients that do not support encryption when accessing SMB data will not be able to access this share.</td>
</tr>
</tbody>
</table>

**Steps**

1. Enter the appropriate command:
If you want to... Enter the command...

Add share properties

```
vservr cifs share properties add -vserver
vserver_name -share-name share_name -share-
properties properties,...
```

Remove share properties

```
vservr cifs share properties remove -vserver
vserver_name -share-name share_name -share-
properties properties,...
```

- `-vserver vserver_name` specifies the name of the Storage Virtual Machine (SVM) that contains the share whose properties you want to modify.
- `-share-name share_name` is the name of the share whose properties you want to modify.
- `-share-properties properties` is the list of share properties you want to add or remove.

2. Verify the share property settings:

```
vservr cifs share show -vserver vserver_name -share-name share_name
```

**Examples**

The following command adds the `showsnapshot` share property to a share named “share1” on SVM vs1:

```
cluster1::> vservr cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot
```

```
cluster1::> vservr cifs share show -vserver vs1
Vserver Share Path Properties Comment ACL
--------- ------ -------- ---------- -------- -----------
vs1 share1 /share1 oplocks - Everyone / Full Control
           browsable
           showsnapshot
```

The following command removes the `browsable` share property from a share named “share2” on SVM vs1:

```
cluster1::> vservr cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable
```

```
cluster1::> vservr cifs share show -vserver vs1
Vserver Share Path Properties Comment ACL
--------- ------ -------- ---------- -------- -----------
vs1 share2 /share2 oplocks - Everyone / Full Control
           changenotify
```

**Related tasks**

- *Creating an SMB share on a CIFS server* on page 177

**Related references**

- *Commands for managing SMB shares* on page 186
Viewing information about SVM shares using the MMC

You can view information about SMB shares on your Storage Virtual Machine (SVM) using the MMC (Microsoft Management Console). Before you can view the shares, you need to connect the MMC to the SVM.

**Steps**

1. To open the MMC on your Windows server, in Windows Explorer, right-click the icon for the local computer, and then select *Manage*.
2. On the left panel, select *Computer Management*.
3. Select *Action > Connect to another computer*.
   The Select Computer dialog box appears.
4. Type the name of the storage system or click *Browse* to locate the storage system.
5. Click *OK*.
   The MMC connects to the SVM.
6. Perform the following:
   a. From the Computer Management page, expand the *System Tools* hierarchy in the left navigation pane.
      An error message displays: The remote procedure call failed and did not execute (1727). The right display pane remains blank. This is a known issue in this version of Data ONTAP.
   b. To work around this issue, click *OK* to close the error box, and then click *System Tools* again.
      The *System Tools* hierarchy expands.
7. In the navigation pane, click *Shared Folders > Shares*.
   A list of shares on the SVM is displayed in the right display pane.
8. To display the share properties for a share, double-click the share to open the *Properties* box.

**Related concepts**

*Managing SMB share-level ACLs* on page 187

**Commands for managing SMB shares**

You use the `vserver cifs share` and `vserver cifs share properties` commands to manage SMB shares.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create an SMB share</td>
<td><code>vserver cifs share create</code></td>
</tr>
<tr>
<td>Display SMB shares</td>
<td><code>vserver cifs share show</code></td>
</tr>
<tr>
<td>Modify an SMB share</td>
<td><code>vserver cifs share modify</code></td>
</tr>
<tr>
<td>Delete an SMB share</td>
<td><code>vserver cifs share delete</code></td>
</tr>
<tr>
<td>Add share properties to an existing share</td>
<td><code>vserver cifs share properties add</code></td>
</tr>
</tbody>
</table>
If you want to...  Use this command...

Remove share properties from an existing share  vserver cifs share properties remove

Display information about share properties  vserver cifs share properties show

See the man page for each command for more information.

Securing file access by using SMB share ACLs

You can secure access to files and folders over a network by configuring share access control lists (ACLs) on SMB shares. Share-level ACLs are used in combination with file-level permissions and, optionally, export policies to determine effective access rights.

You can use either domain or local users or groups when configuring ACLs.

Related concepts

How Data ONTAP secures file and directory access on page 24
Securing file access by using Storage-Level Access Guard on page 152
Securing file access by using file permissions on page 190
Securing file access by using Dynamic Access Control (DAC) on page 196

Related tasks

Creating an SMB share on a CIFS server on page 177
Creating SMB share access control lists on page 188
Performing security traces on page 285

Managing SMB share-level ACLs

You can change share-level ACLs to give users more or less access rights to the share. You can configure share-level ACLs by using either Windows users and groups or UNIX users and groups.

After you create a share, by default, the share-level ACL gives read access to the standard group named Everyone. Read access in the ACL means that all users in the domain and all trusted domains have read-only access to the share.

You can change a share-level ACL by using the Microsoft Management Console (MMC) on a Windows client or the Data ONTAP command line.

The following guidelines apply when you use the MMC:

• The user and group names specified must be Windows names.
• You can specify only Windows permissions.

The following guidelines apply when you use the Data ONTAP command line:

• The user and group names specified can be Windows names or UNIX names.
  If a user and group type is not specified when creating or modifying ACLs, the default type is Windows users and groups.
• You can specify only Windows permissions.

Related tasks

Viewing information about SVM shares using the MMC on page 186
How Data ONTAP uses share-level ACLs

A share-level ACL consists of a list of access control entries (ACEs). Each ACE contains a user or group name and a set of permissions that determines user or group access to the share, regardless of the security style of the volume or qtree containing the share.

When an SMB user tries to access a share, Data ONTAP always checks the share-level ACL (access control list) to determine whether access should be granted.

A share-level ACL only restricts access to files in the share; it never grants more access than the file-level ACLs.

Creating SMB share access control lists

Configuring share permissions by creating access control lists (ACLs) for SMB shares enables you to control the level of access to a share for users and groups.

About this task

You can configure share-level ACLs by using local or domain Windows user or group names or UNIX user or group names.

• If you specify a domain Windows user name, you must include the user's domain using the format domain\username.

• The value for the user-or-group parameter is case-insensitive text.

The value for the -permission parameter can be one of the following:

• No_access
• Read
• Change
• Full_Control

Steps

1. Configure the ACL:

<table>
<thead>
<tr>
<th>If you want to configure ACLs by using a...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows user</td>
<td>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_domain_name \user_name -permission access_right</td>
</tr>
<tr>
<td>Windows group</td>
<td>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_group_name -permission access_right</td>
</tr>
<tr>
<td>UNIX user</td>
<td>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type unix-user -user-or-group UNIX_user_name -permission access_right</td>
</tr>
</tbody>
</table>
If you want to configure ACLs by using a...

Enter the command...

| UNIX group | vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type unix-group -user-or-group UNIX_group_name -permission access_right |

2. Verify that the ACL applied to the share is correct by using the `vserver cifs share access-control show` command.

The following command gives Change permissions to the “salesteam” Windows group for the “sales” share on the “vs1” Storage Virtual Machine (SVM):

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share sales -user-or-group salesteam -permission Change
```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Share</th>
<th>User/Group</th>
<th>User/Group Name</th>
<th>Type</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>c$</td>
<td>BUILTIN\Administrators</td>
<td>windows</td>
<td>Full_Control</td>
<td></td>
</tr>
<tr>
<td>vs1</td>
<td>sales</td>
<td>salesteam</td>
<td>windows</td>
<td>Change</td>
<td></td>
</tr>
</tbody>
</table>

The following command gives Read permission to the “engineering” UNIX group for the “eng” share on the “vs2” SVM:

```
cluster1::> vserver cifs share access-control create -vserver vs2 -share eng -user-group-type unix-group -user-or-group eng -permission Read
```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Share</th>
<th>User/Group</th>
<th>User/Group Name</th>
<th>Type</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs2</td>
<td>c$</td>
<td>BUILTIN\Administrators</td>
<td>windows</td>
<td>Full_Control</td>
<td></td>
</tr>
<tr>
<td>vs2</td>
<td>eng</td>
<td>engineering</td>
<td>unix-group</td>
<td>Read</td>
<td></td>
</tr>
</tbody>
</table>

The following commands give Change permission to the local Windows group named “group1” and Full_Control permission to the local Windows user named “user1” for the “datavol5” share on the “vs1” SVM:

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share datavol5 -user-group-type windows -user-or-group group1 -permission Change
cluster1::> vserver cifs share access-control create -vserver vs1 -share datavol5 -user-group-type windows -user-or-group user1 -permission Full_Control
```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Share</th>
<th>User/Group</th>
<th>User/Group Name</th>
<th>Type</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>c$</td>
<td>BUILTIN\Administrators</td>
<td>windows</td>
<td>Full_Control</td>
<td></td>
</tr>
<tr>
<td>vs1</td>
<td>datavol5</td>
<td>group1</td>
<td>windows</td>
<td>Change</td>
<td></td>
</tr>
<tr>
<td>vs1</td>
<td>datavol5</td>
<td>user1</td>
<td>windows</td>
<td>Full_Control</td>
<td></td>
</tr>
</tbody>
</table>

Related tasks:

*Creating an SMB share on a CIFS server* on page 177
Commands for managing SMB share access control lists

You need to know the commands for managing SMB access control lists (ACLs), which includes creating, displaying, modifying, and deleting them.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a new ACL</td>
<td>vserver cifs share access-control create</td>
</tr>
<tr>
<td>Display ACLs</td>
<td>vserver cifs share access-control show</td>
</tr>
<tr>
<td>Modify an ACL</td>
<td>vserver cifs share access-control modify</td>
</tr>
<tr>
<td>Delete an ACL</td>
<td>vserver cifs share access-control delete</td>
</tr>
</tbody>
</table>

Securing file access by using file permissions

You can secure access by configuring file permissions on files and folders contained within the share through which SMB clients access data. File-level permissions are used in combination with share-level ACLs and, optionally, export policies to determine effective access rights. Files and folders might be secured with NTFS permissions or UNIX permissions.

If files and folders are secured with UNIX file permissions, then the mapped UNIX user and the UNIX user’s groups are used to evaluate file permissions.

Related concepts

- How security styles affect data access on page 20
- How name mapping is used to secure SMB file access on SVMs with FlexVol volumes on page 23
- How Data ONTAP secures file and directory access on page 24
- Securing file access by using SMB share ACLs on page 187
- How UNIX file permissions provide access control when accessing files over SMB on page 196
- Securing file access by using Storage-Level Access Guard on page 152
- Securing file access by using Dynamic Access Control (DAC) on page 196

Related tasks

- Performing security traces on page 285

Configuring standard NTFS file permissions by using the Windows Security tab

You can configure standard NTFS file permissions on files and directories by using the Windows Security tab in the Windows Properties window. This is the same method used when configuring standard file permissions on data residing on a Windows client.

Before you begin

The administrator performing this task must have sufficient NTFS permissions to change permissions on the selected objects.

About this task

Configuring NTFS file permissions is done by adding entries to NTFS discretionary access control lists (DACLs) that are associated with an NTFS security descriptor. The security descriptor is then applied to NTFS files and directories. These tasks are automatically handled by the Windows GUI.
The security descriptor can contain DACLs for applying file and folder access permissions, security access control lists (SACLs) for file and folder auditing, or both SACLs and DACLs.

You can set standard NTFS file permissions for file and folder access by completing the following steps on a Windows host:

**Steps**

1. From the **Tools** menu in Windows Explorer, select **Map network drive**.

2. Complete the **Map Network Drive** box:
   a. Select a **Drive** letter.
   b. In the **Folder** box, type the CIFS server name containing the share that contains the data to which you want to apply permissions and the name of the share.

   **Example**
   If your CIFS server name is CIFS_SERVER and your share is named “share1”, you would enter `\CIFS_SERVER\share1`.

   **Note:** You can specify the IP address of the data interface for the CIFS server instead of the CIFS server name.
   c. Click **Finish**.

   The drive you selected is mounted and ready with the Windows Explorer window displaying files and folders contained within the share.

3. Select the file or directory for which you want to set NTFS file permissions.

4. Right-click the file or directory, and then select **Properties**.

5. Select the **Security** tab.

   The Security tab displays the list of users and groups for which NTFS permission are set. The Permissions for <Object> box displays a list of Allow and Deny permissions in effect for the selected user or group.

6. Click **Edit**.

   The Permissions for <Object> box opens.

7. Perform the desired actions:

<table>
<thead>
<tr>
<th>If you want to:</th>
<th>Do the following...</th>
</tr>
</thead>
</table>
   | Set standard NTFS permissions for a new user or group | a. Click **Add**.  
The Select User, Computers, Service Accounts, or Groups window opens.  
b. In the **Enter the object names to select** box, type the name of the user or group on which you want to add NTFS permission.  
c. Click **OK**. |

8. Perform the desired actions:
If you want to... | Do the following
--- | ---
Set standard NTFS permissions for a new or existing user or group | In the Permissions for <Object> box, select the Allow or Deny boxes for the type of access that you want to allow or not allow for the selected user or group.
Remove a user or group | Click Remove.

Standard permissions are compilations of the more granular advanced access rights. You can set the following types of standard permissions:

- Full control
- Modify
- Read & Execute
- List folder contents
- Read
- Write

Note: If some or all of the standard permission boxes are not selectable, it is because the permissions are inherited from the parent object. The Special permissions box is not selectable. If it is selected, it means that one or more of the granular advanced rights has been set for the selected user or group.

9. After you finish adding, removing, or editing NTFS permissions on that object, click OK.

For more information about how to set standard NTFS permissions, see your Windows documentation.

Related tasks

- Configuring and applying file security on NTFS files and folders using the CLI on page 255
- Displaying information about file security on NTFS security-style volumes on page 242
- Displaying information about file security on mixed security-style volumes on page 244
- Displaying information about file security on UNIX security-style volumes on page 246

Configuring advanced NTFS file permissions using the Windows Security tab

You can configure standard NTFS file permissions on files and folders by using the Windows Security tab in the Windows Properties window.

Before you begin

The administrator performing this task must have sufficient NTFS permissions to change permissions on the selected objects.

About this task

Configuring NTFS file permissions is done on a Windows host by adding entries to NTFS discretionary access control lists (DACLs) that are associated with an NTFS security descriptor. The security descriptor is then applied to NTFS files and directories. These tasks are automatically handled by the Windows GUI.

Steps

1. From the Tools menu in Windows Explorer, select Map network drive.
2. Complete the Map Network Drive dialog box:
   a. Select a Drive letter.
   b. In the Folder box, type the CIFS server name containing the share that contains the data to which you want to apply permissions and the name of the share.

   **Example**
   If your CIFS server name is “CIFS_SERVER” and your share is named “share1”, you should type `\CIFS_SERVER\share1`.

   **Note:** You can specify the IP address of the data interface for the CIFS server instead of the CIFS server name.
   c. Click Finish.

   The drive you selected is mounted and ready with the Windows Explorer window displaying files and folders contained within the share.

3. Select the file or directory for which you want to set NTFS file permissions.

4. Right-click the file or directory, and then select Properties.

5. Select the Security tab.

   The Security tab displays the list of users and groups for which NTFS permission are set. The Permissions for box displays a list of Allow and Deny permissions in effect for each user or group selected.

6. Click Advanced.

   The Windows Properties window displays information about existing file permissions assigned to users and groups.

7. Click Change Permissions.

   The Permissions window opens.

8. Perform the desired actions:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Do the following...</th>
</tr>
</thead>
</table>
   | Set up advanced NTFS permissions for a new user or group | a. Click Add.  
   | | b. In the **Enter the object name to select** box, type the name of the user or group that you want to add.  
   | | c. Click OK. |
   | Change advanced NTFS permissions from a user or group | a. In the **Permissions entries** box, select the user or group whose advanced permissions you want to change.  
   | | b. Click Edit. |
   | Remove advanced NTFS permissions for a user or group | a. In the **Permissions entries** box, select the user or group that you want to remove.  
   | | b. Click Remove.  
   | | c. Skip to Step 13. |

If you are adding advanced NTFS permissions on a new user or group or changing NTFS advanced permissions on an existing user or group, the Permission Entry for `<Object>` box opens.
9. In the **Apply to** box, select how you want to apply this NTFS file permission entry. You can select one of the following:
   - This folder, subfolders and files
   - This folder and subfolders
   - This folder only
   - This folder and files
   - Subfolders and files only
   - Subfolders only
   - Files only

   If you are setting up NTFS file permissions on a single file, the **Apply to** box is not active. The **Apply to** setting defaults to **This object only**.

10. In the **Permissions** box, select the **Allow** or **Deny** boxes for the advanced permissions that you want to set on this object.

   • To allow the specified access, select the **Allow** box.
   • To not allow the specified access, select the **Deny** box.

   You can set permissions on the following advanced rights:

   • **Full control**
     If you choose this advanced right, all other advanced rights are automatically chosen (either Allow or Deny rights).

   • **Traverse folder / execute file**
   • **List folder / read data**
   • **Read attributes**
   • **Read extended attributes**
   • **Create files / write data**
   • **Create folders / append data**
   • **Write attributes**
   • **Write extended attributes**
   • **Delete subfolders and files**
   • **Delete**
   • **Read permissions**
   • **Change permissions**
   • **Take ownership**

   **Note:** If any of the advanced permission boxes are not selectable, it is because the permissions are inherited from the parent object.

11. If you want subfolders and files of this object to inherit these permissions, select the **Apply these permissions to objects and/or containers within this container only** box.
12. Click OK.

13. After you finish adding, removing, or editing NTFS permissions, specify the inheritance setting for this object:

   - Select the **Include inheritable permissions from this object's parent** box.
     This is the default.

   - Select the **Replace all child object permissions with inheritable permissions from this object** box.
     This setting is not present in the Permissions box if you are setting NTFS file permissions on a single file.

     **Note:** Be cautious when selecting this setting. This setting removes all existing permissions on all child objects and replaces them with this object's permission settings. You could inadvertently remove permissions that you did not want removed. It is especially important when setting permissions in a mixed security-style volume or qtree. If child objects have a UNIX effective security style, propagating NTFS permissions to those child objects results in Data ONTAP changing these objects from UNIX security style to NTFS security style, and all UNIX permissions on those child objects are replaced with NTFS permissions.

   - Select both boxes.

   - Select neither box.

14. Click OK to close the Permissions box.

15. Click OK to close the **Advanced Security settings for <Object>** box.

   For more information about how to set advanced NTFS permissions, see your Windows documentation.

**Related tasks**

- Configuring and applying file security on NTFS files and folders using the CLI on page 255
- Displaying information about file security on NTFS security-style volumes on page 242
- Displaying information about file security on mixed security-style volumes on page 244
- Displaying information about file security on UNIX security-style volumes on page 246

**How to configure NTFS file permissions using the Data ONTAP CLI**

You can configure NTFS file permissions on files and directories using the Data ONTAP CLI. This enables you to configure NTFS file permissions without needing to connect to the data using an SMB share on a Windows Client.

You can configure NTFS file permissions by adding entries to NTFS discretionary access control lists (DACLs) that are associated with an NTFS security descriptor. The security descriptor is then applied to NTFS files and directories.

You can only configure NTFS file permissions using the command line. You cannot configure NFSv4 ACLs by using the CLI.

**Related tasks**

- Configuring and applying file security on NTFS files and folders using the CLI on page 255
How UNIX file permissions provide access control when accessing files over SMB

A FlexVol volume can have one of three types of security style: NTFS, UNIX, or mixed. You can access data over SMB regardless of security style; however, appropriate UNIX file permissions are needed to access data with UNIX effective security.

When data is accessed over SMB, there are several access controls used when determining whether a user is authorized to perform a requested action:

- Export permissions
  Configuring export permissions for SMB access is optional in Data ONTAP 8.2 and later releases.

- Share permissions

- File permissions
  The following types of file permissions might be applied to the data on which the user wants to perform an action:
  - NTFS
  - UNIX NFSv4 ACLs
  - UNIX mode bits

For data with NFSv4 ACLs or UNIX mode bits set, UNIX style permissions are used to determine file access rights to the data. The SVM administrator needs to set the appropriate file permission to ensure that users have the rights to perform the desired action.

**Note:** Data in a mixed security-style volume might have either NTFS or UNIX effective security style. If the data has UNIX effective security style, then NFSv4 permissions or UNIX mode bits are used when determining file access rights to the data.

Securing file access by using Dynamic Access Control (DAC)

You can secure access by using Dynamic Access Control and by creating central access policies in Active Directory and applying them to files and folders on Storage Virtual Machines (SVMs) through applied Group Policy Objects (GPOs). You can configure auditing to use central access policy staging events to see the effects of changes to central access policies before you apply them.

Additions to CIFS credentials

Before Dynamic Access Control, a CIFS credential included a security principal's (the user's) identity and Windows group membership. With Dynamic Access Control, three more types of information are added to the credential—device identity, device claims, and user claims:

- Device identity
  The analog of the user's identity information, except it is the identity and group membership of the device that the user is logging in from.

- Device claims
  Assertions about a device security principal. For example, a device claim might be that it is a member of a specific OU.

- User claims
  Assertions about a user security principal. For example, a user claim might be that their AD account is a member of a specific OU.
Additions to security descriptor

Dynamic Access Control support includes the addition of three new ACE types defined by Microsoft for security descriptors:

- Conditional ACEs, which are conditional expressions that give the administrator a high level of control over access to a resource. Conditional ACEs can be included in the DACL or the SACL.
- Resource ACEs, which allow you to associate arbitrary attributes with a file or directory. Attributes are defined in AD, and are represented as name/value pairs in the ACE. For example, a file can be tagged as being owned by the marketing department using this mechanism. These ACEs are only present in the SACL.
- Policy ACEs, which tie central access policies to the resource. Policy ACEs contain a SID that can be used to look up an access policy that is then used for additional access checks. These ACEs are only present in the SACL. This enables an administrator to change access to a resource with a simple change in Active Directory.

Central access policies

Central access policies for files enable organizations to centrally deploy and manage authorization policies that include conditional expressions using user groups, user claims, device claims, and resource properties.

For example, for accessing high business impact data, a user needs to be a full time employee and only have access to the data from a managed device. Central access policies are defined in Active Directory and distributed to file servers via the GPO mechanism.

Central access policy staging with advanced auditing

Central access policies can be “staged”, in which case they are evaluated in a “what-if” manner during file access checks. The results of what would have happened if the policy was in effect and how that differs from what is currently configured are logged as an audit event. In this way, administrators can use audit event logs to study the impact of an access policy change before actually putting the policy in play. After evaluating the impact of an access policy change, the policy can be deployed via GPOs to the desired SVMs.

Related concepts

- Supported GPOs on page 113
- Applying Group Policy Objects to CIFS servers on page 113
- Auditing NAS events on SVMs with FlexVol volumes on page 421

Related tasks

- Enabling or disabling GPO support on a CIFS server on page 118
- Displaying information about GPO configurations on page 120
- Displaying information about central access policies on page 125
- Displaying information about central access policy rules on page 126
- Configuring central access policies to secure data on CIFS servers on page 200
- Displaying information about Dynamic Access Control security on page 203
- Performing security traces on page 285
- Creating a file and directory auditing configuration on SVMs on page 436

Related information

- Clustered Data ONTAP 8.3.1 man page: vserver security file-directory show - Display file/folder security information
Supported Dynamic Access Control functionality

If you want to use Dynamic Access Control (DAC) on your CIFS server, you need to understand how clustered Data ONTAP supports Dynamic Access Control functionality in Active Directory environments.

Supported for Dynamic Access Control

Clustered Data ONTAP supports the following functionality when Dynamic Access Control is enabled on the CIFS server:

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Claims into the file system</td>
<td>Claims are simple name and value pairs that state some truth about a user. User credentials now contain claim information, and security descriptors on files can perform access checks that include claims checks. This gives administrators a finer level of control over who can access files.</td>
</tr>
<tr>
<td>Conditional expressions to file access checks</td>
<td>When modifying the security parameters of a file, users can now add arbitrarily complex conditional expressions to the file's security descriptor. The conditional expression can include checks for claims.</td>
</tr>
<tr>
<td>Central control of file access via central access policies</td>
<td>Central access policies are a kind of ACL stored in Active Directory that can be tagged to a file. Access to the file is only granted if the access checks of both the security descriptor on disk and the tagged central access policy allows access. This gives administrators the ability to control access to files from a central location (AD) without having to modify the security descriptor on disk.</td>
</tr>
<tr>
<td>Central access policy staging</td>
<td>Adds the ability to try out security changes without affecting actual file access, by “staging” a change to the central access policies, and seeing the effect of the change in an audit report.</td>
</tr>
<tr>
<td>Support for displaying information about central access policy security by using the clustered Data ONTAP CLI</td>
<td>Extends the vserver security file-directory show command to display information about applied central access policies.</td>
</tr>
<tr>
<td>Security tracing that includes central access policies</td>
<td>Extends the vserver security trace command family to display results that include information about applied central access policies.</td>
</tr>
</tbody>
</table>

Unsupported for Dynamic Access Control

Clustered Data ONTAP does not support the following functionality when Dynamic Access Control is enabled on the CIFS server:

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic classification of NTFS file system objects</td>
<td>This is an extension to the Windows File Classification Infrastructure that is not supported in clustered Data ONTAP.</td>
</tr>
</tbody>
</table>
### Functionality vs. Comments

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced auditing other than central access policy staging</td>
<td>Only central access policy staging is supported for advanced auditing.</td>
</tr>
</tbody>
</table>

### Considerations when using Dynamic Access Control and central access policies with CIFS servers

There are certain considerations you must keep in mind when using Dynamic Access Control (DAC) and central access policies to secure files and folders on CIFS servers.

**NFS access can be denied to root if policy rule applies to domain\administrator user**

Under certain circumstances, NFS access to root might be denied when central access policy security is applied to the data that the root user is attempting to access. The issue occurs when the central access policy contains a rule that is applied to the domain\administrator and the root account is mapped to the domain\administrator account.

Instead of applying a rule to the domain\administrator user, you should apply the rule to a group with administrative privileges, such as the domain\administrators group. In this way, you can map root to the domain\administrator account without root being impacted by this issue.

**CIFS server’s BUILTIN\Administrators group has access to resources when the applied central access policy is not found in Active Directory**

It is possible that resources contained within the CIFS server have central access policies applied to them, but when the CIFS server uses the central access policy’s SID to attempt to retrieve information from Active Directory, the SID does not match any existing central access policy SIDs in Active Directory. Under these circumstances, the CIFS server applies the local default recovery policy for that resource.

The local default recovery policy allows the CIFS server’s BUILTIN\Administrators group access to that resource.

### Enabling or disabling Dynamic Access Control

The option that enables you to use Dynamic Access Control (DAC) to secure objects on your CIFS server is disabled by default. You must enable the option if you want to use Dynamic Access Control on your CIFS server. If you later decide that you do not want to use Dynamic Access Control to secure objects stored on the CIFS server, you can disable the option.

**About this task**

Once Dynamic Access Control is enabled, the file system can contain ACLs with Dynamic Access Control-related entries. If Dynamic Access Control is disabled, the current Dynamic Access Control entries will be ignored, and new ones will not be allowed.

This option is available only at the advanced privilege level.

**Steps**

1. Set the privilege level to advanced:

   ```bash
   set -privilege advanced
   ```

2. Perform one of the following actions:
If you want Dynamic Access Control to be...

<table>
<thead>
<tr>
<th>Enabled</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>vserver cifs options modify -vserver vserver_name -is-dac-enabled true</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Disabled</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>vserver cifs options modify -vserver vserver_name -is-dac-enabled false</td>
</tr>
</tbody>
</table>

3. Return to the administrator privilege level:

```
set -privilege admin
```

Related tasks

- Configuring central access policies to secure data on CIFS servers on page 200

Managing ACLs that contain Dynamic Access Control ACEs when Dynamic Access Control is disabled

If you have resources that have ACLs applied with Dynamic Access Control ACEs and you disable Dynamic Access Control on the Storage Virtual Machine (SVM), you must remove the Dynamic Access Control ACEs before you can manage the non-Dynamic Access Control ACEs on that resource.

About this task

After Dynamic Access Control is disabled, you cannot remove existing non-Dynamic Access Control ACEs or add new non-Dynamic Access Control ACEs until you have removed the existing Dynamic Access Control ACEs.

You can use whichever tool you normally use to manage ACLs to perform these steps.

Steps

1. Determine what Dynamic Access Control ACEs are applied to the resource.
2. Remove the Dynamic Access Control ACEs from the resource.
3. Add or remove non-Dynamic Access Control ACEs as desired from the resource.

Configuring central access policies to secure data on CIFS servers

There are several steps that you must take to secure access to data on the CIFS server using central access policies, including enabling Dynamic Access Control (DAC) on the CIFS server, configuring central access policies in Active Directory, applying the central access policies to Active Directory containers with GPOs, and enabling GPOs on the CIFS server.

Before you begin

- The Active Directory must be configured to use central access policies.
- You must have sufficient access on the Active Directory domain controllers to create central access policies and to create and apply GPOs to the containers that contain the CIFS servers.
- You must have sufficient administrative access on the Storage Virtual Machine (SVM) to execute the necessary commands.
About this task

Central access policies are defined and applied to group policy objects (GPOs) on Active Directory. You can consult the Microsoft TechNet Library for instructions about configuring central access policies and GPOs.

Microsoft TechNet Library

Steps

1. Enable Dynamic Access Control on the SVM if it is not already enabled by using the `vserver cifs options modify` command.

   **Example**
   ```
   vserver cifs options modify -vserver vs1 -is-dac-enabled true
   ```

2. Enable group policy objects (GPOs) on the CIFS server if they are not already enabled by using the `vserver cifs group-policy modify` command.

   **Example**
   ```
   vserver cifs group-policy modify -vserver vs1 -status enabled
   ```

3. Create central access rules and central access policies on Active Directory.

4. Create a group policy object (GPO) to deploy the central access policies on Active Directory.

5. Apply the GPO to the container where the CIFS server computer account is located.

6. Manually update the GPOs applied to the CIFS server by using the `vserver cifs group-policy update` command.

   **Example**
   ```
   vserver cifs group-policy update -vserver vs1
   ```

7. Verify that the GPO central access policy is applied to the resources on the CIFS server by using the `vserver cifs group-policy show-applied` command.

   **Example**
   ```
   The following example shows that the Default Domain Policy has two central access policies that are applied to the CIFS server:
   vserver cifs group-policy show-applied
   ```

   ```
   Vserver: vs1
   --------------------------
   GPO Name: Default Domain Policy
   Level: Domain
   Status: enabled
   Advanced Audit Settings:
   Object Access:
       Central Access Policy Staging: failure
   Registry Settings:
   Refresh Time Interval: 22
   Refresh Random Offset: 8
   Hash Publication Mode for BranchCache: per-share
   Hash Version Support for BranchCache: all-versions
   Security Settings:
   Event Audit and Event Log:
       Audit Logon Events: none
       Audit Object Access: success
   Log Retention Method: overwrite-as-needed
   ```
Max Log Size: 16384
File Security:
/voll/home
/voll/dir1
Kerberos:
Max Clock Skew: 5
Max Ticket Age: 10
Max Renew Age: 7
Privilege Rights:
Take Ownership: usr1, usr2
Security Privilege: usr1, usr2
Change Notify: usr1, usr2
Registry Values:
Signing Required: false
Restrict Anonymous:
No enumeration of SAM accounts: true
No enumeration of SAM accounts and shares: false
Restrict anonymous access to shares and named pipes: true
Combined restriction for anonymous user: no-access
Restricted Groups:
gpr1
gpr2
Central Access Policy Settings:
Policies: cap1
cap2

GPO Name: Resultant Set of Policy
Level: RSOP
Advanced Audit Settings:
Object Access:
Central Access Policy Staging: failure
Registry Settings:
Refresh Time Interval: 22
Refresh Random Offset: 8
Hash Publication Mode for BranchCache: per-share
Hash Version Support for BranchCache: all-versions
Security Settings:
Event Audit and Event Log:
Audit Logon Events: none
Audit Object Access: success
Log Retention Method: overwrite-as-needed
Max Log Size: 16384
File Security:
/voll/home
/voll/dir1
Kerberos:
Max Clock Skew: 5
Max Ticket Age: 10
Max Renew Age: 7
Privilege Rights:
Take Ownership: usr1, usr2
Security Privilege: usr1, usr2
Change Notify: usr1, usr2
Registry Values:
Signing Required: false
Restrict Anonymous:
No enumeration of SAM accounts: true
No enumeration of SAM accounts and shares: false
Restrict anonymous access to shares and named pipes: true
Combined restriction for anonymous user: no-access
Restricted Groups:
gpr1
gpr2
Central Access Policy Settings:
Policies: cap1
cap2
2 entries were displayed.
You can display information about Dynamic Access Control (DAC) security on NTFS volumes and on data with NTFS effective security on mixed security-style volumes. This includes information about conditional ACEs, resource ACEs, and central access policy ACEs. You can use the results to validate your security configuration or to troubleshoot file access issues.

About this task

You must supply the name of the Storage Virtual Machine (SVM) and the path to the data whose file or folder security information you want to display. You can display the output in summary form or as a detailed list.

Step

1. Display file and directory security settings with the desired level of detail:

<table>
<thead>
<tr>
<th>If you want to display information...</th>
<th>Enter the following command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>In summary form</td>
<td><code>vserver security file-directory show -vserver vserver_name -path path</code></td>
</tr>
<tr>
<td>With expanded detail</td>
<td><code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code></td>
</tr>
<tr>
<td>Where output is displayed with group and user SIDs</td>
<td><code>vserver security file-directory show -vserver vserver_name -path path -lookup-names false</code></td>
</tr>
</tbody>
</table>

Examples

The following example displays Dynamic Access Control security information about the path `/vol1` in SVM vs1:

```bash
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
Vserver: vs1
  File Path: /vol1
  File Inode Number: 112
  Security Style: mixed
  Effective Style: ntfs
  DOS Attributes: 10
  DOS Attributes in Text: ----D---
  Expanded Dos Attribute: -
  Unix User Id: 0
  Unix Group Id: 1
  Unix Mode Bits: 777
  Unix Mode Bits in Text: rwxrwxrwx
  ACLs: NTFS Security Descriptor
    Control:0x8bf14
    Owner:CIFS\Administrator
    Group:CIFS\Domain Admins
    DACL - ACEs
      ALL-Everyone-0xf01ff-OI|CI|SA|FA
      RESOURCE ATTRIBUTE-Everyone-0x0
      ("Department_MS",TS,0x10020,"Finance")
      POLICY ID-All resources - No Write-0x0-0I|CI
    DACL - ACEs
      ALLOW-CIFS\Administrator-0x1f01ff-0I|CI
      ALLOW-Everyone-0x1f01ff-0I|CI
```
Related tasks

Displaying information about GPO configurations on page 120
Displaying information about central access policies on page 125
Displaying information about central access policy rules on page 126

Revert considerations for Dynamic Access Control

You should be aware of what happens when reverting to a version of Data ONTAP that does not support Dynamic Access Control (DAC) and what you must do before and after reverting.

If you want to revert the cluster to a version of clustered Data ONTAP that does not support Dynamic Access Control and Dynamic Access Control is enabled on one or more the Storage Virtual Machines (SVMs), you must do the following before reverting:

• You must disable Dynamic Access Control on all SVMs that have it enabled on the cluster.
• You must modify any auditing configurations on the cluster that contain the cap-staging event type to use only the file-op event type.

You must understand and act on some important revert considerations for files and folders with Dynamic Access Control ACEs:

• If the cluster is reverted, existing Dynamic Access Control ACEs are not removed; however, they will be ignored in file access checks.
• Since Dynamic Access Control ACEs are ignored after reversion, access to files will change on files with Dynamic Access Control ACEs.
  This could allow users to access files they previously could not, or not be able to access files that they previously could.
• You should apply non-Dynamic Access Control ACEs to the affected files to restore their previous level of security.
  This can be done either before reverting or immediately after reversion completes.

  Note: Since Dynamic Access Control ACEs are ignored after reversion, it is not required that you remove them when applying non-Dynamic Access Control ACEs to the affected files. However, if desired, you can manually remove them.

Where to find additional information about configuring and using Dynamic Access Control and central access policies

Additional resources are available to help you configure and use Dynamic Access Control and central access policies.

You can find information about how to configure Dynamic Access Control and central access policies on Active Directory in the Microsoft TechNet Library.

Microsoft TechNet: Dynamic Access Control Scenario Overview
Microsoft TechNet: Central Access Policy Scenario

The following references can help you configure the CIFS server to use and support Dynamic Access Control and central access policies:

Using GPOs on the CIFS server

Applying Group Policy Objects to CIFS servers on page 113
Securing SMB access using export policies

You can optionally use export policies to restrict SMB access to files and folders on Storage Virtual Machine (SVM) volumes. You can use export policies in combination with share-level and file-level permissions to determine effective access rights.

For information about configuring and managing export policies, see the Clustered Data ONTAP File Access Management Guide for NFS.

Related concepts

Role that export policies play with SMB access on page 24
Creating and configuring SMB shares on page 172
Securing file access by using SMB share ACLs on page 187
Securing file access by using file permissions on page 190

How export policies are used with SMB access

If export policies for SMB access are enabled on the CIFS server, export policies are used when controlling access to Storage Virtual Machine (SVM) volumes or qtrees by SMB clients. To access data, you can create an export policy that allows SMB access and then associate the policy with the volumes or qtrees containing SMB shares.

An export policy has one or more rules applied to it that specifies which clients are allowed access to the data and what authentication protocols are supported for read-only and read-write access. You can configure export policies to allow access over SMB to all clients, a subnet of clients, or a specific client and to allow authentication using Kerberos authentication, NTLM authentication, or both Kerberos and NTLM authentication when determining read-only and read-write access to data.

After processing all export rules applied to the export policy, Data ONTAP can determine whether the client is granted access and what level of access is granted. Export rules apply to client machines, not to Windows users and groups. Export rules do not replace Windows user and group-based authentication and authorization. Export rules provide another layer of access security in addition to share and file-access permissions.

You associate exactly one export policy with each volume to configure client access to the volume. Each SVM can contain multiple export policies. This enables you to do the following for SVMs with multiple volumes:

• Assign different export policies to each volume of the SVM for individual client access control to each volume in the SVM.
• Assign the same export policy to multiple volumes of the SVM for identical client access control without having to create a new export policy for each volume.

You associate exactly one export policy to each volume or qtree to configure client access to the volume or qtree. Each SVM can contain multiple export policies. This enables you to do the following for SVMs with multiple volumes or qtrees:

• Assign different export policies to each volume or qtree of the SVM for individual client access control to each volume or qtree in the SVM.
• Assign the same export policy to multiple volumes or qtrees of the SVM for identical client access control without having to create a new export policy for each volume or qtree.
Each SVM has at least one export policy called “default”, which contains no rules. You cannot delete this export policy, but you can rename or modify it. Each volume on the SVM by default is associated with the default export policy. If export policies for SMB access is disabled on the SVM, the “default” export policy has no effect on SMB access.

You can configure rules that provide access to both NFS and SMB hosts and associate that rule with an export policy, which can then be associated with the volume or qtree that contains data to which both NFS and SMB hosts need access. Alternatively, if there are some volumes or qtrees where only SMB clients require access, you can configure an export policy with rules that only allow access using the SMB protocol and that uses only Kerberos or NTLM (or both) for authentication for read-only and write access. The export policy is then associated to the volumes or qtrees where only SMB access is desired.

If export policies for SMB is enabled and a client makes an access request that is not permitted by the applicable export policy, the request fails with a permission-denied message. If a client does not match any rule in the volume's export policy, then access is denied. If an export policy is empty, then all accesses are implicitly denied. This is true even if the share and file permissions would otherwise permit access. This means that you must configure your export policy to minimally allow the following on volumes or qtrees containing SMB shares:

- Allow access to all clients or the appropriate subset of clients
- Allow access over SMB
- Allow appropriate read-only and write access by using Kerberos or NTLM authentication (or both)

For information about configuring and managing export policies, see the *Clustered Data ONTAP File Access Management Guide for NFS*.

**Related concepts**

- What happens to existing SMB export policies when upgrading on page 206
- How export rules work on page 208

**Related tasks**

- Enabling or disabling export policies for SMB access on page 207

**Related references**

- Examples of export policy rules that restrict or allow access over SMB on page 209

**What happens to existing SMB export policies when upgrading**

For releases earlier than Data ONTAP 8.2, SMB export policies are mandatory. Starting with Data ONTAP 8.2, export policies for SMB access are optional and are disabled by default. You need to be aware of what happens when upgrading from releases where export policies are mandatory.

If you upgrade from a version of Data ONTAP where configured export policies were mandatory for SMB access and the cluster contains Storage Virtual Machines (SVMs) with CIFS servers, support for export policies is enabled for those SVMs after the upgrade. You do not need to reconfigure SMB access for existing CIFS servers when upgrading.

If you create a new SVM and CIFS server on the upgraded cluster, export policies for the new CIFS server are disabled by default. You can enable and configure export policies on the new CIFS servers if desired.
Enabling or disabling export policies for SMB access

You can enable or disable export policies for SMB access on Storage Virtual Machines (SVMs). Using export policies to control SMB access to resources is optional for Data ONTAP 8.2 and later.

Before you begin

The following are the requirements for enabling export policies for SMB:

- The client must have a “PTR” record in DNS before you create the export rules for that client.
- An additional set of “A” and “PTR” records for host names is required if the SVM provides access to NFS clients and the host name you want to use for NFS access is different from the CIFS server name.

About this task

Starting with Data ONTAP 8.2, a new option controls whether export policies are enabled for SMB access. When setting up a new CIFS server on your SVM, the usage of export policies for SMB access is disabled by default. You can enable export policies for SMB access if you want to control access based on authentication protocol or on client IP addresses or host names. You can enable or disable export policies for SMB access at any time.

When upgrading a cluster from versions of Data ONTAP earlier than 8.2, this option is automatically enabled on CIFS servers in the cluster that are using export policies to control SMB access. There is no unexpected change to configured access controls when you upgrade to a version of Data ONTAP where export policies for SMB access is optional.

Steps

1. Set the privilege level to advanced:
   
   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want export policies to be...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled true</td>
</tr>
<tr>
<td>Disabled</td>
<td>vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled false</td>
</tr>
</tbody>
</table>

3. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Example

The following example enables the usage of export policies to control SMB client access to resources on SVM vs1:

```bash
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y
```
cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy-enabled true
cluster1::*> set -privilege admin

Related concepts

*How export policies are used with SMB access* on page 205

**How export rules work**

Export rules are the functional elements of an export policy. Export rules match client access requests to a volume or qtree against specific parameters you configure to determine how to handle the client access requests.

An export policy must contain at least one export rule to allow access to clients. If an export policy contains more than one rule, the rules are processed in the order in which they appear in the export policy. The rule order is dictated by the rule index number. If a rule matches a client, the permissions of that rule are used and no further rules are processed. If no rules match, the client is denied access.

You can configure export rules to determine client access permissions using the following criteria:

- The file access protocol used by the client sending the request, for example, NFSv4 or SMB.
- A client identifier, for example, host name or IP address.
- The security type used by the client to authenticate, for example, Kerberos v5, NTLM, or AUTH_SYS.

If a rule specifies multiple criteria, and the client does not match one or more of them, the rule does not apply.

**Example**

The export policy contains an export rule with the following parameters:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

The client access request is sent using the NFSv3 protocol and the client has the IP address 10.1.17.37.

Even though the client access protocol matches, the IP address of the client is in a different subnet from the one specified in the export rule. Therefore, client matching fails and this rule does not apply to this client.

**Example**

The export policy contains an export rule with the following parameters:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`
The client access request is sent using the NFSv4 protocol and the client has the IP address 10.1.16.54.

The client access protocol matches and the IP address of the client is in the specified subnet. Therefore, client matching is successful and this rule applies to this client. The client gets read-write access regardless of its security type.

### Example

The export policy contains an export rule with the following parameters:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

Client #1 has the IP address 10.1.16.207, sends an access request using the NFSv3 protocol, and authenticated with Kerberos v5.

Client #2 has the IP address 10.1.16.211, sends an access request using the NFSv3 protocol, and authenticated with AUTH_SYS.

The client access protocol and IP address matches for both clients. The read-only parameter allows read-only access to all clients regardless of the security type they authenticated with. Therefore both clients get read-only access. However, only client #1 gets read-write access because it used the approved security type Kerberos v5 to authenticate. Client #2 does not get read-write access.

### Related references

*Examples of export policy rules that restrict or allow access over SMB* on page 209

### Examples of export policy rules that restrict or allow access over SMB

The examples show how to create export policy rules that restrict or allow access over SMB on a Storage Virtual Machine (SVM) that has export policies for SMB access enabled.

Export policies for SMB access are disabled by default. You need to configure export policy rules that restrict or allow access over SMB only if you have enabled export policies for SMB access.

### Export rule for SMB access only

The following command creates an export rule on the SVM named “vs1” that has the following configuration:

- Policy name: cifs1
- Index number: 1
- Client match: Matches only clients on the 192.168.1.0/24 network
- Protocol: Only enables SMB access
- Read-only access: To clients using NTLM or Kerberos authentication
- Read-write access: To clients using Kerberos authentication
Export rule for SMB and NFS access

The following command creates an export rule on the SVM named “vs1” that has the following configuration:

- Policy name: cifsnfs1
- Index number: 2
- Client match: Matches all clients
- Protocol: SMB and NFS access
- Read-only access: To all clients
- Read-write access: To all clients using Kerberos (NFS and SMB) or NTLM authentication (SMB)
- Mapping for UNIX user ID 0 (zero): Mapped to user ID 65534 (which typically maps to the user name nobody)
- Suid and sgid access: Allows

Export rule for SMB access using NTLM only

The following command creates an export rule on the SVM named “vs1” that has the following configuration:

- Policy name: ntlm1
- Index number: 1
- Client match: Matches all clients
- Protocol: Only enables SMB access
- Read-only access: Only to clients using NTLM
- Read-write access: Only to clients using NTLM

**Note:** If you configure the read-only option or the read-write option for NTLM-only access, you must use IP address-based entries in the client match option. Otherwise, you receive access denied errors. This is because Data ONTAP uses Kerberos Service Principal Names (SPN) when using a host name to check on the client’s access rights. NTLM authentication does not support SPN names.

For information about configuring and managing export policies, see the *Clustered Data ONTAP File Access Management Guide for NFS.*

**Related concepts**

*How export rules work* on page 208
Considerations when reverting export policies for SMB

For releases earlier than Data ONTAP 8.2, SMB export policies are mandatory. Starting with Data ONTAP 8.2, export policies for SMB access are optional and are disabled by default. There are certain considerations when reverting to a release where export policies are mandatory.

There are two scenarios where export policies for SMB access are a consideration when reverting to a version of Data ONTAP where export policies for SMB are mandatory:

- You have a cluster with an installed version of Data ONTAP where the use of export policies for SMB is optional and export policies are disabled on all Storage Virtual Machines (SVMs). In this case, the SVMs and contained volumes do not have export policies that allow SMB access. If you revert to a version of Data ONTAP where export policies are mandatory, export policies are turned on and required for SMB access. This results in denial of access to SMB clients. The recommendation is that you configure export policies for SMB on all SVMs before you revert so that there are no hard-to-resolve SMB client access issues after the revert.

- You have a cluster with an installed version of Data ONTAP where the use of export policies for SMB access is optional and export policies for SMB are enabled on some but not all of the SVMs. If you revert to a version of Data ONTAP where export policies are mandatory, export policies are turned on and required for SMB access for all SVMs. This results in denial of access to SMB clients on SVMs where export policies were not previously enabled. The recommendation is that you configure export policies for SMB on all SVMs before you revert so that there are no hard-to-resolve SMB client access issues after the revert.

**Note:** If you upgraded from a version of Data ONTAP where export policies are mandatory, export policies for SMB were automatically enabled on existing SVMs. Even if you subsequently disabled export policies for SMB on those existing SVMs, the export policies remain in place. Upon a revert back to a version of Data ONTAP where export policies are mandatory, the existing export policies are used to determine SMB access. However, before reverting, you should create export policies for SMB access on any new SVMs created after the initial upgrade.
Managing file access using SMB

After you create and configure a CIFS server on your Storage Virtual Machine (SVM) and set up file access over SMB shares, there are a number of tasks you might want to perform to manage file access.

Using local users and groups for authentication and authorization

You can create local users and groups on the Storage Virtual Machine (SVM). The CIFS server can use local users for CIFS authentication and can use both local users and groups for authorization when determining both share and file and directory access rights.

Local group members can be local users, domain users and groups, and domain machine accounts. Local users and groups can also be assigned privileges. Privileges control access to SVM resources and can override the permissions that are set on objects. A user or member of a group that is assigned a privilege is granted the specific rights that the privilege allows.

Note: Privileges do not provide clustered Data ONTAP general administrative capabilities.

Related concepts

What local privileges are on page 216
Enabling or disabling local users and groups functionality on page 219
Managing local user accounts on page 221
Managing local groups on page 227
Managing local privileges on page 234

How Data ONTAP uses local users and groups

When configuring and using local users and groups, you must understand what they are and how they are used. For example, you can use local users and groups to provide share and file-access security to data residing on the Storage Virtual Machine (SVM). You can also assign user management rights to users through the use of local users and groups.

Local users and groups concepts

You should know what local users and groups are, and some basic information about them, before determining whether to configure and use local users and groups in your environment.

Local user

A user account with a unique security identifier (SID) that has visibility only on the Storage Virtual Machine (SVM) on which it is created. Local user accounts have a set of attributes, including user name and SID. A local user account authenticates locally on the CIFS server using NTLM authentication.

User accounts have several uses:

• Used to grant User Rights Management privileges to a user.

• Used to control share-level and file-level access to file and folder resources that the SVM owns.

Local group
A group with a unique SID has visibility only on the SVM on which it is created. Groups contain a set of members. Members can be local users, domain users, domain groups, and domain machine accounts. Groups can be created, modified, or deleted.

Groups have several uses:

- Used to grant User Rights Management privileges to its members.
- Used to control share-level and file-level access to file and folder resources that the SVM owns.

**Local domain**

A domain that has local scope, which is bounded by the SVM. The local domain's name is the CIFS server name. Local users and groups are contained within the local domain.

**Security identifier (SID)**

A SID is a variable-length numeric value that identifies Windows-style security principals. For example, a typical SID takes the following form:

S-1-5-21-3139654847-1303905135-2517279418-123456.

**NTLM authentication**

A Microsoft Windows security method used to authenticate users on a CIFS server.

**Cluster replicated database (RDB)**

A replicated database with an instance on each node in a cluster. Local user and group objects are stored in the RDB.

**Reasons for creating local users and groups**

There are several reasons for creating local users and groups on your Storage Virtual Machine (SVM). For example, you can access the CIFS server using a local user account if the domain controllers are unavailable, or you may want to use local groups to assign privileges.

You can create one or more local user accounts for the following reasons:

- You want the ability to authenticate and log in to the CIFS server if domain controllers are unavailable.
  
  Local users can authenticate with the CIFS server using NTLM authentication when the domain controller is down or when network problems prevent your CIFS server from contacting the domain controller.

- You want to assign a local user User Rights Management privileges.
  
  User Rights Management is the ability for a CIFS server administrator to control what rights users and groups have on the SVM. You can assign privileges to a user by assigning the privileges to the user's account or by making the user a member of a local group that has those privileges.

  **Note:** Although a local user can authenticate locally, the CIFS server is not operating in Workgroup mode. Workgroup mode is not supported in this version of Data ONTAP. The CIFS server must still be part of an Active Directory domain. The CIFS server is operating as a member server in an Active Directory domain.

You might want to create one or more local groups for the following reasons:

- You want to control access to file and folder resources by using local groups for share and file-access control.

- You want to create local groups with customized User Rights Management privileges.
  
  There are certain built-in user groups with predefined privileges. To assign a customized set of privileges, you can create a local group and assign that group the necessary privileges. You can then add local users, domain users, and domain groups to the local group.
How local user authentication works

Before a local user can access data on a CIFS server, the user must create an authenticated session. Because SMB is session-based, the identity of the user can be determined just once, when the session is first set up. The CIFS server uses NTLM-based authentication when authenticating local users. Both NTLMv1 and NTLMv2 are supported.

Data ONTAP uses local authentication under three use cases. Each use case depends on whether the domain portion of the user name (with the DOMAIN\user format) matches the CIFS server’s local domain name (the CIFS server name):

- **The domain portion matches**
  Users who provide local user credentials when requesting access to data are authenticated locally on the CIFS server.

- **The domain portion does not match**
  Data ONTAP attempts to use NTLM authentication with a domain controller in the domain to which the CIFS server belongs. If authentication succeeds, the login is complete. If it does not succeed, what happens next depends on why authentication did not succeed. For example, if the user exists in Active Directory but the password is invalid or expired, Data ONTAP does not attempt to use the corresponding local user account on the CIFS server. Instead, authentication fails. There are other cases where Data ONTAP uses the corresponding local account on the CIFS server, if it exists, for authentication—even though the NetBIOS domain names do not match. For example, if a matching domain account exists but it is disabled, Data ONTAP uses the corresponding local account on the CIFS server for authentication.

- **The domain portion is not specified**
  Data ONTAP first attempts authentication as a local user. If authentication as a local user fails, then Data ONTAP authenticates the user with a domain controller in the domain to which the CIFS server belongs.

After local or domain user authentication is completed successfully, Data ONTAP constructs a complete user access token, which takes into account local group membership and privileges.

For more information about NTLM authentication for local users, see the Microsoft Windows documentation.

Related tasks

*Enabling or disabling local user authentication* on page 220

How user access tokens are constructed

When a user maps a share, an authenticated SMB session is established and a user access token is constructed that contains information about the user, the user’s group membership and cumulative privileges, and the mapped UNIX user.

Unless the functionality is disabled, local user and group information is also added to the user access token. The way access tokens are constructed depends on whether the login is for a local user or an Active Directory domain user:

- **Local user login**
  Although local users can be members of different local groups, local groups cannot be members of other local groups. The local user access token is composed of a union of all privileges assigned to groups to which a particular local user is a member.
• Domain user login
When a domain user logs in, Data ONTAP obtains a user access token that contains the user SID and SIDs for all the domain groups to which the user is a member. Data ONTAP uses the union of the domain user access token with the access token provided by local memberships of the user’s domain groups (if any), as well as any direct privileges assigned to the domain user or any of its domain group memberships.

For both local and domain user login, the Primary Group RID is also set for the user access token. The default RID is Domain Users (RID 513). This default RID cannot be changed in this version of Data ONTAP.

The Windows-to-UNIX and UNIX-to-Windows name mapping process follows the same rules for both local and domain accounts.

Note: There is no implied, automatic mapping from a UNIX user to a local account. If this is required, an explicit mapping rule must be specified using the existing name mapping commands.

Considerations when using SnapMirror on SVMs that contain local groups
There are certain considerations you should keep in mind if you configure SnapMirror on volumes owned by Storage Virtual Machines (SVMs) that contain local groups.

You cannot use local groups in ACEs applied to files, directories, or shares that are replicated by SnapMirror to another SVM. If you use the SnapMirror feature to create a DR mirror to a volume on another SVM and the volume has an ACE for a local group, the ACE is not valid on the mirror. If data is replicated to a different SVM, the data is effectively crossing into a different local domain. The permissions granted to local users and groups are valid only within the scope of the SVM on which they were originally created.

What happens to local users and groups when deleting CIFS servers
The default set of local users and groups is created when a CIFS server is created, and they are associated with the Storage Virtual Machine (SVM) hosting the CIFS server. SVM administrators can create local users and groups at any time. You need to be aware of what happens to local users and groups when you delete the CIFS server.

Local users and groups are associated with SVMs; therefore, they are not deleted when CIFS servers are deleted due to security considerations. Although local users and groups are not deleted when the CIFS server is deleted, they are hidden. You cannot view or manage local users and groups until you re-create a CIFS server on the SVM.

Note: The CIFS server administrative status does not affect visibility of local users or groups.

How you can use Microsoft Management Console with local users and groups
You can view information about local users and groups from the Microsoft Management Console. With this release of Data ONTAP, you cannot perform other management tasks for local users and groups from the Microsoft Management Console.

Considerations when reverting
If you plan to revert the cluster to a Data ONTAP release that does not support local users and groups and local users and groups are being used to manage file access or user rights, you must be aware of certain considerations.

• Due to security reasons, information about configured local users, groups, and privileges are not deleted when Data ONTAP is reverted to a version that does not support local users and groups functionality.

• Upon a revert to a prior major version of Data ONTAP, Data ONTAP does not use local users and groups during authentication and credential creation.
• Local users and groups are not removed from file and folder ACLs.
• File access requests that depend on access being granted because of permissions granted to local users or groups are denied.

To allow access, you must reconfigure file permissions to allow access based on domain objects instead of local user and group objects.

**What local privileges are**

Privileges are well-known rights that can be granted to local and domain users and groups to perform *User Rights Management* tasks on the CIFS server. You cannot create privileges. You can only add or remove existing privileges.

**List of supported privileges**

Data ONTAP has a predefined set of supported privileges. Certain predefined local groups have some of these privileges added to them by default. You can also add or remove privileges from the predefined groups or create new local users or groups and add privileges to the groups that you created or to existing domain users and groups.

The following table lists the supported privileges on the Storage Virtual Machine (SVM) and provides a list of BUILTIN groups with assigned privileges:

<table>
<thead>
<tr>
<th>Privilege name</th>
<th>Default security setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SeTcbPrivilege</td>
<td>None</td>
<td>Act as part of the operating system</td>
</tr>
<tr>
<td>SeBackupPrivilege</td>
<td>BUILTIN\Administrators,</td>
<td>Back up files and directories, overriding any ACLs</td>
</tr>
<tr>
<td></td>
<td>BUILTIN\Backup Operators</td>
<td></td>
</tr>
<tr>
<td>SeRestorePrivilege</td>
<td>BUILTIN\Administrators,</td>
<td>Restore files and directories, overriding any ACLs</td>
</tr>
<tr>
<td></td>
<td>BUILTIN\Backup Operators</td>
<td></td>
</tr>
<tr>
<td>SeTakeOwnershipPrivilege</td>
<td>BUILTIN\Administrators</td>
<td>Take ownership of files or other objects</td>
</tr>
<tr>
<td>SeSecurityPrivilege</td>
<td>BUILTIN\Administrators</td>
<td>Manage auditing This includes viewing, dumping, and clearing the security log.</td>
</tr>
<tr>
<td>SeChangeNotifyPrivilege</td>
<td>BUILTIN\Administrators,</td>
<td>Bypass traverse checking Users with this privilege are not required to have traverse (x) permissions to traverse folders, symlinks, or junctions.</td>
</tr>
<tr>
<td></td>
<td>BUILTIN\Backup Operators, BUILTIN\Power Users, BUILTIN\Users, Everyone</td>
<td></td>
</tr>
</tbody>
</table>

**Related concepts**

*Managing local privileges* on page 234

*Configuring bypass traverse checking* on page 237
How to assign privileges

You can assign privileges directly to local users or domain users. Alternatively, you can assign users to local groups whose assigned privileges match the capabilities that you want those users to have.

- You can assign a set of privileges to a group that you create. You then add a user to the group that has the privileges that you want that user to have.
- You can also assign local users and domain users to predefined groups whose default privileges match the privileges that you want to grant to those users.

Related concepts

*Configuring bypass traverse checking* on page 237

Related tasks

*Adding privileges to local or domain users or groups* on page 234
*Removing privileges from local or domain users or groups* on page 235
*Resetting privileges for local or domain users and groups* on page 236

Requirements and considerations

Before you create and configure local users and groups on your CIFS server, you need to be aware of certain requirements and considerations.

Considerations when using BUILTIN groups and the local administrator account

There are certain considerations you should keep in mind when you use BUILTIN groups and the local administrator account. For example, you should know that you can rename the local administrator account, but you cannot delete this account.

- The Administrator account can be renamed but cannot be deleted.
- The Administrator account cannot be removed from the BUILTIN\Administrators group.
- BUILTIN groups can be renamed but cannot be deleted.
  After the BUILTIN group is renamed, another local object can be created with the well-known name; however, the object is assigned a new RID.
- There is no local Guest account.

Related references

*Predefined BUILTIN groups and default privileges* on page 218

Requirements for local user passwords

By default, local user passwords must meet complexity requirements. The password complexity requirements are similar to the requirements defined in the Microsoft Windows *Local security policy.* The password must meet the following criteria:

- Must be at least six characters in length
- Must not contain the user account name
- Must contain characters from at least three of the following four categories:
  - English uppercase characters (A through Z)
Predefined BUILTIN groups and default privileges

You can assign membership of a local user or domain user to a predefined set of BUILTIN groups provided by Data ONTAP. Predefined groups have predefined privileges assigned.

The following table describes the predefined groups:

<table>
<thead>
<tr>
<th>Predefined BUILTIN group</th>
<th>Default privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>BUILTIN\Administrators RID 544</td>
<td>• SeBackupPrivilege</td>
</tr>
<tr>
<td></td>
<td>• SeRestorePrivilege</td>
</tr>
<tr>
<td></td>
<td>• SeSecurityPrivilege</td>
</tr>
<tr>
<td></td>
<td>• SeTakeOwnershipPrivilege</td>
</tr>
<tr>
<td></td>
<td>• SeChangeNotifyPrivilege</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>BUILTIN\Power Users RID 547</td>
<td>SeChangeNotifyPrivilege</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>BUILTIN\Backup Operators RID 551</td>
<td>• SeBackupPrivilege</td>
</tr>
<tr>
<td></td>
<td>• SeRestorePrivilege</td>
</tr>
<tr>
<td></td>
<td>• SeChangeNotifyPrivilege</td>
</tr>
<tr>
<td>Predefined BUILTIN group</td>
<td>Default privileges</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>BUILTIN\Users</td>
<td>SeChangeNotifyPrivilege</td>
</tr>
<tr>
<td>RID 545</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When first created, this group does not have any members (besides the implied Authenticated Users special group). When the SVM is joined to a domain, the domain\Domain Users group is added to this group. If the SVM leaves the domain, the domain\Domain Users group is removed from this group.</td>
</tr>
<tr>
<td>Everyone</td>
<td>SeChangeNotifyPrivilege</td>
</tr>
<tr>
<td>SID S-1-1-0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This group includes all users, including guests (but not anonymous users). This is an implied group with an implied membership.</td>
</tr>
</tbody>
</table>

**Related concepts**

- Considerations when using BUILTIN groups and the local administrator account on page 217
- Configuring bypass traverse checking on page 237

**Related references**

- List of supported privileges on page 216

### Enabling or disabling local users and groups functionality

Before you can use local users and groups for access control of NTFS security-style data, local user and group functionality must be enabled. Additionally, if you want to use local users for SMB authentication, the local user authentication functionality must be enabled.

Local users and groups functionality and local user authentication are enabled by default. If they are not enabled, you must enable them before you can configure and use local users and groups. You can disable local users and groups functionality at any time.

In addition to explicitly disabling local user and group functionality, Data ONTAP disables local user and group functionality if any node in the cluster is reverted to a Data ONTAP release that does not support the functionality. Local user and group functionality is not enabled until all nodes in the cluster are running a version of Data ONTAP that supports it.

**Related concepts**

- Managing local user accounts on page 221
- Managing local groups on page 227
- Managing local privileges on page 234

### Enabling or disabling local users and groups

You can enable or disable local users and groups for SMB access on Storage Virtual Machines (SVMs). Local users and groups functionality is enabled by default.

**About this task**

You can use local users and groups when configuring SMB share and NTFS file permissions and can optionally use local users for authentication when creating an SMB connection. To use local users for authentication, you must also enable the local users and groups authentication option.
Steps

1. Set the privilege level to advanced:
   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:
   
<table>
<thead>
<tr>
<th>If you want local users and groups to be...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>vserver cifs options modify -vserver vserver_name -is-local-users-and-groups-enabled true</td>
</tr>
<tr>
<td>Disabled</td>
<td>vserver cifs options modify -vserver vserver_name -is-local-users-and-groups-enabled false</td>
</tr>
</tbody>
</table>

3. Return to the admin privilege level:
   ```
   set -privilege admin
   ```

Example

The following example enables local users and groups functionality on SVM vs1:

```bash
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y
cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and-groups-enabled true
cluster1::*> set -privilege admin
```

Related tasks

- **Enabling or disabling local user authentication** on page 220
- **Enabling or disabling local user accounts** on page 224

Enabling or disabling local user authentication

You can enable or disable local user authentication for SMB access on Storage Virtual Machines (SVMs). The default is to allow local user authentication, which is useful when the SVM cannot contact a domain controller or if you choose not to use domain-level access controls.

Before you begin

Local users and groups functionality must be enabled on the CIFS server.

About this task

You can enable or disable local user authentication at any time. If you want to use local users for authentication when creating an SMB connection, you must also enable the CIFS server's local users and groups option.

Steps

1. Set the privilege level to advanced:
   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:
If you want local authentication to be...

<table>
<thead>
<tr>
<th>Enabled</th>
<th><code>vserver cifs options modify -vserver vserver_name -is-local-auth-enabled true</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td><code>vserver cifs options modify -vserver vserver_name -is-local-auth-enabled false</code></td>
</tr>
</tbody>
</table>

3. Return to the admin privilege level:

   `set -privilege admin`

**Example**

The following example enables local user authentication on SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y
cluster1::>* vserver cifs options modify -vserver vs1 -is-local-auth-enabled true
cluster1::>* set -privilege admin
```

**Related concepts**

- *How local user authentication works* on page 214

**Related tasks**

- *Enabling or disabling local users and groups* on page 219

**Managing local user accounts**

You can manage local user accounts by creating, modifying, and deleting them, and by displaying information about user accounts and group membership. You can also perform other management tasks, such as enabling, disabling, and renaming user accounts, setting the password for an account, and managing local account password complexity.

**Related concepts**

- *Managing local groups* on page 227
- *Managing local privileges* on page 234

**Creating local user accounts**

You can create a local user account that can be used to authorize access to data contained in the Storage Virtual Machine (SVM) over an SMB connection. You can also use local user accounts for authentication when creating an SMB session.

**Before you begin**

Local users and groups functionality must be enabled.

**About this task**

When you create a local user account, you must specify a user name and you must specify the SVM with which to associate the account. The user name must meet the following requirements:
• Must not exceed 20 characters
• Cannot be terminated by a period
• Cannot include commas
• Cannot include any of the following printable characters:
  " / \ ] : | < > + = ; * @
• Cannot include characters in the ASCII range 1-31, which are non-printable

You can optionally specify the following parameters:

• -full-name user_name specifies the user’s full name.
  If the full name contains a space, it must be enclosed within quotation marks.

• -description text specifies a description for the local user.
  If the description contains a space, it must be enclosed within quotation marks.

• -is account-disabled {true|false} specifies if the user account is enabled or disabled.
  By default, the user account is enabled.

Steps

1. Create the local user by entering the following command:

   vserver cifs users-and-groups local-user create -vserver vserver_name
   user-name user_name optional_parameters

   The command prompts for the local user’s password.

2. Enter a password for the local user and confirm the password.

   The password must meet the following requirements:
   • Must be at least six characters in length
   • Must not contain the user account name
   • Must contain characters from at least three of the following four categories:
     ◦ English uppercase characters (A through Z)
     ◦ English lowercase characters (a through z)
     ◦ Base 10 digits (0 through 9)
     ◦ Special characters: ~, !, @, #, 0, ^, &, *, _, -, +, =, `\, |, (, ), [, ], : ; , "', <, >, .., ?, /

3. Verify that the user has been successfully created:

   vserver cifs users-and-groups local-user show -vserver vserver_name

Example

The following example creates a local user “CIFS_SERVER\sue” associated with SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user create -vserver vs1 -user-name CIFS_SERVER\sue
Enter the password:
Enter the password:
```

```
cluster1::> vserver cifs users-and-groups local-user show
```
Modifying local user accounts

You can modify a local user account if you want to change an existing user's full name or description, and if you want to enable or disable the user account. You can also rename a local user account if the user's name is compromised or if a name change is needed for administrative purposes.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Enter the command...</th>
</tr>
</thead>
</table>
| Modify the local user's full name | `vserver cifs users-and-groups local-user modify`  
`-vserver vserver_name -user-name user_name`  
`-full-name text`  
If the full name contains a space, then it must be enclosed within double quotation marks. |
| Modify the local user's description | `vserver cifs users-and-groups local-user modify`  
`-vserver vserver_name -user-name user_name`  
`-description text`  
If the description contains a space, then it must be enclosed within double quotation marks. |
| Enable or disable the local user account | `vserver cifs users-and-groups local-user modify`  
`-vserver vserver_name -user-name user_name -is-account-disabled {true|false}` |
| Rename the local user account | `vserver cifs users-and-groups local-user rename`  
`-vserver vserver_name -user-name user_name -new-user-name new_user_name`  
The new user name must meet the following criteria:  
- Must not exceed 20 characters  
- Cannot be terminated by a period  
- Cannot include commas  
- Cannot include any of the following printable characters:  
  `" / \ [ ] : | < > = ; ? * @`  
- Cannot include characters in the ASCII range 1-31, which are non-printable  
When renaming a local user, the new user name must remain associated with the same CIFS server as the old user name. |

Example

The following example renames the local user “CIFS_SERVER\sue” to “CIFS_SERVER\sue_new” on Storage Virtual Machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```
Enabling or disabling local user accounts

You enable a local user account if you want the user to be able to access data contained in the Storage Virtual Machine (SVM) over an SMB connection. You can also disable a local user account if you do not want that user to access SVM data over SMB.

About this task

You enable a local user by modifying the user account.

Step

1. Perform the appropriate action:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the user account</td>
<td><code>vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account-disabled false</code></td>
</tr>
<tr>
<td>Disable the user account</td>
<td><code>vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account-disabled true</code></td>
</tr>
</tbody>
</table>

Changing local user account passwords

You can change a local user's account password. This can be useful if the user's password is compromised or if the user has forgotten the password.

Step

1. Change the password by performing the appropriate action:

   `vserver cifs users-and-groups local-user set-password -vserver vserver_name -user-name user_name`

   The password must meet the following criteria:
   - Must be at least six characters in length
   - Must not contain the user account name
   - Must contain characters from at least three of the following four categories:
     - English uppercase characters (A through Z)
     - English lowercase characters (a through z)
     - Base 10 digits (0 through 9)
     - Special characters: `~ ! @ # $ % ^ & * ( ) [ ] : ; " ' < > , . ? /`

Example

The following example sets the password for the local user “CIFS_SERVER\sue” associated with Storage Virtual Machine (SVM, formerly known as Vserver) vs1:
cluster1::> vserver cifs users-and-groups local-user set-password -user-name CIFS_SERVER\sue -vserver vs1

Enter the new password:
Confirm the new password:

Related tasks

*Enabling or disabling required password complexity for local SMB users* on page 80
*Displaying information about CIFS server security settings* on page 79

Displaying information about local users

You can display a list of all local users in a summary form. If you want to determine which account settings are configured for a specific user, you can display detailed account information for that user as well as the account information for multiple users. This information can help you determine if you need to modify a user's settings, and also to troubleshoot authentication or file access issues.

About this task

Information about a user's password is never displayed.

Step

1. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information about all users on the Storage Virtual Machine (SVM)</td>
<td>vserver cifs users-and-groups local-user show -vserver vserver_name</td>
</tr>
<tr>
<td>Display detailed account information for a user</td>
<td>vserver cifs users-and-groups local-user show -instance -vserver vserver_name -user-name user_name</td>
</tr>
</tbody>
</table>

There are other optional parameters that you can choose when you run the command. See the man page for more information.

Example

The following example displays information about all local users on SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver User Name                     Full Name       Description
-------- --------------------------- ------------- --------------
vs1      CIFS_SERVER\Administrator   James Smith     Built-in administrator account
vs1      CIFS_SERVER\sue            Sue Jones       
```

Displaying information about group memberships for local users

You can display information about which local groups that a local user belongs to. You can use this information to determine what access the user should have to files and folders. This information can be useful in determining what access rights the user should have to files and folders or when troubleshooting file access issues.

About this task

You can customize the command to display only the information that you want to see.
Step

1. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display local user membership information for a specified local user</td>
<td><code>vserver cifs users-and-groups local-user show-membership -user-name user_name</code></td>
</tr>
<tr>
<td>Display local user membership information for the local group of which this local user is a member</td>
<td><code>vserver cifs users-and-groups local-user show-membership -membership group_name</code></td>
</tr>
<tr>
<td>Display user membership information for local users that are associated with a specified Storage Virtual Machine (SVM)</td>
<td><code>vserver cifs users-and-groups local-user show-membership -vserver vserver_name</code></td>
</tr>
<tr>
<td>Display detailed information for all local users on a specified SVM</td>
<td><code>vserver cifs users-and-groups local-user show-membership -instance -vserver vserver_name</code></td>
</tr>
</tbody>
</table>

Example

The following example displays the membership information for all local users on SVM vs1; user “CIFS_SERVER\Administrator” is a member of the “BUILTIN\Administrators” group, and “CIFS_SERVER\sue” is a member of “CIFS_SERVER\g1” group:

```
cluster1::> vserver cifs users-and-groups local-user show-membership -vserver vs1

<table>
<thead>
<tr>
<th>Vserver</th>
<th>User Name</th>
<th>Membership</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>CIFS_SERVER\Administrator</td>
<td>BUILTIN\Administrators</td>
</tr>
<tr>
<td></td>
<td>CIFS_SERVER\sue</td>
<td>CIFS_SERVER\g1</td>
</tr>
</tbody>
</table>
```

Deleting local user accounts

You can delete local user accounts from your Storage Virtual Machine (SVM) if they are no longer needed for local SMB authentication to the CIFS server or for determining access rights to data contained on your SVM.

About this task

Keep the following in mind when deleting local users:

- The file system is not altered.
  Windows Security Descriptors on files and directories that refer to this user are not adjusted.
- All references to local users are removed from the membership and privileges databases.
- Standard, well-known users such as Administrator cannot be deleted.

Steps

1. Determine the name of the local user account that you want to delete:

```
vserver cifs users-and-groups local-user show -vserver vserver_name
```

2. Delete the local user:
3. Verify that the user account is deleted:

```
vserver cifs users-and-groups local-user show -vserver vserver_name
```

**Example**

The following example deletes the local user “CIFS_SERVER\sue” associated with SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1 -user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>User Name</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>CIFS_SERVER\Administrator</td>
<td>James Smith</td>
<td>Built-in administrator account</td>
</tr>
<tr>
<td>vs1</td>
<td>CIFS_SERVER\sue</td>
<td>Sue Jones</td>
<td></td>
</tr>
</tbody>
</table>

**Managing local groups**

You can manage local groups by creating or modifying groups, displaying information about groups and group membership, and by deleting unneeded groups. You can also perform other management tasks, such as renaming groups and adding or removing both local and domain users from the local groups.

**Related concepts**

- *Managing local user accounts* on page 221
- *Managing local privileges* on page 234

**Creating local groups**

You can create local groups that can be used for authorizing access to data associated with the Storage Virtual Machine (SVM) over an SMB connection. You can also assign privileges that define what user rights or capabilities a member of the group has.

**Before you begin**

The local users and groups functionality is enabled.

**About this task**

Keep the following in mind when creating local groups:

- You can specify a group name with or without the local domain name.

  The local domain is the CIFS server name on the SVM. For example, if the CIFS server name is “CIFS_SERVER” and you want to create the “engineering” group, you can specify the group name as “engineering” or “CIFS_SERVER\engineering”.

  The following rules apply when using a local domain as part of the group name:

  - You can only specify the local domain name for the SVM to which the group is applied.
    For example, if the local CIFS server name is “CIFS_SERVER”, you cannot specify the following local group name: “CORP_SERVER\group1”.
  - You cannot use the *BUILTIN* term as a local domain in the group name.
    For example, you cannot create a group named “BUILTIN\group1”.

...
You cannot specify a group name that already exists.

When you create a local group, you must specify a name for the group and you must specify the SVM with which to associate the group. You can optionally specify a description for the local group. The group name must meet the following requirements:

- Must not exceed 256 characters
- Cannot be terminated by a period
- Cannot include commas
- Cannot include any of the following printable characters:
  " / \ [ ] : | < > + = ; ? * @
- Cannot include characters in the ASCII range 1-31, which are non-printable

Steps

1. Create the local group by entering the following command:

   ```
   vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name
   ```

2. Verify that the group is successfully created:

   ```
   vserver cifs users-and-groups local-group show -vserver vserver_name
   ```

Example

The following example creates a local group “CIFS_SERVER\engineering” associated with SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group create -vserver vs1 -group-name CIFS_SERVER\engineering
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Group Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>BUILTIN\Administrators</td>
<td>Built-in Administrators group</td>
</tr>
<tr>
<td>vs1</td>
<td>BUILTIN\Backup Operators</td>
<td>Backup Operators group</td>
</tr>
<tr>
<td>vs1</td>
<td>BUILTIN\Power Users</td>
<td>Restricted administrative privileges</td>
</tr>
<tr>
<td>vs1</td>
<td>BUILTIN\Users</td>
<td>All users</td>
</tr>
<tr>
<td>vs1</td>
<td>CIFS_SERVER\engineering</td>
<td>All users</td>
</tr>
<tr>
<td>vs1</td>
<td>CIFS_SERVER\sales</td>
<td>All users</td>
</tr>
</tbody>
</table>

Modifying local groups

You can modify existing local groups by changing the description for an existing local group or by renaming the group.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify the local group description</td>
<td>vserver cifs users-and-groups local-group modify -vserver vserver_name -group-name group_name -description text</td>
</tr>
</tbody>
</table>

If the description contains a space, then it must be enclosed within double quotation marks.
If you want to... | Use the command...
---|---
Rename the local group | `vserver cifs users-and-groups local-group rename -vserver vserver_name -group-name group_name -new-group-name new_group_name`

The new group name must meet the following criteria:
- Must not exceed 256 characters
- Cannot be terminated by a period
- Cannot include commas
- Cannot include any of the following printable characters: "/\[]:<>+=?@"
- Cannot include characters in the ASCII range 1-31, which are non-printable

**Examples**

The following example renames the local group “CIFS_SERVER\engineering” to “CIFS_SERVER\engineering_new”:

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1 -group-name CIFS_SERVER\engineering -new-group-name CIFS_SERVER\engineering_new
```

The following example modifies the description of the local group “CIFS_SERVER\engineering”:

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1 -group-name CIFS_SERVER\engineering -description "New Description"
```

**Displaying information about local groups**

You can display a list of all local groups configured on the cluster or on a specified Storage Virtual Machine (SVM). This information can be useful when troubleshooting file-access issues to data contained on the SVM or user-rights (privilege) issues on the SVM.

**Step**

1. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want information about...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>All local groups on the cluster</td>
<td><code>vserver cifs users-and-groups local-group show</code></td>
</tr>
<tr>
<td>All local groups on the SVM</td>
<td><code>vserver cifs users-and-groups local-group show -vserver vserver_name</code></td>
</tr>
</tbody>
</table>

There are other optional parameters that you can choose when you run this command. See the man page for more information.

**Example**

The following example displays information about all local groups on SVM vs1:
Managing local group membership

You can manage local group membership by adding and removing local or domain users, or adding and removing domain groups. This is useful if you want to control access to data based on access controls placed on the group or if you want users to have privileges associated with that group.

If you no longer want a local user, domain user, or domain group to have access rights or privileges based on membership in a group, you can remove the member from the group.

You must keep the following in mind when adding members to a local group:

• You cannot add users to the special Everyone group.
• The local group must exist before you can add a user to it.
• The user must exist before you can add the user to a local group.
• You cannot add a local group to another local group.
• To add a domain user or group to a local group, Data ONTAP must be able to resolve the name to a SID.

You must keep the following in mind when removing members from a local group:

• You cannot remove members from the special Everyone group.
• The group from which you want to remove a member must exist.
• Data ONTAP must be able to resolve the names of members that you want to remove from the group to a corresponding SID.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a member to a group</td>
<td><code>vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,....]</code></td>
</tr>
<tr>
<td>Remove a member from a group</td>
<td><code>vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,....]</code></td>
</tr>
</tbody>
</table>

Examples

The following example adds a local user “CIFS_SERVER\sue” and a domain group “AD_DOM\dom_eng” to the local group “CIFS_SERVER\engineering” on Storage Virtual Machine (SVM, formerly known as Vserver) vs1:
The following example removes the local users “CIFS_SERVER\sue” and “CIFS_SERVER\james” from the local group “CIFS_SERVER\engineering” on SVM vs1:

```bash
cluster1::> vserver cifs users-and-groups local-group remove-members -vserver vs1 -group-name CIFS_SERVER\engineering -member-names CIFS_SERVER\sue,CIFS_SERVER\james
```

**Related tasks**

*Displaying information about members of local groups* on page 231

**Displaying information about members of local groups**

You can display a list of all members of local groups configured on the cluster or on a specified Storage Virtual Machine (SVM). This information can be useful when troubleshooting file-access issues or user-rights (privilege) issues.

**Step**

1. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want to display information about...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Members of all local groups on the cluster</td>
<td><code>vserver cifs users-and-groups local-group show-members</code></td>
</tr>
<tr>
<td>Members of all local groups on the SVM</td>
<td><code>vserver cifs users-and-groups local-group show-members -vserver vserver_name</code></td>
</tr>
</tbody>
</table>

**Example**

The following example displays information about members of all local groups on SVM vs1:

```bash
cluster1::> vserver cifs users-and-groups local-group show-members -vserver vs1
Vserver Group Name                   Members
--------- ---------------------------- ------------------------
vs1       BUILTIN\Administrators       CIFS_SERVER\Administrator
          AD_DOMAIN\Domain Admins
          AD_DOMAIN\dom_grp1
          BUILTIN\Users          AD_DOMAIN\Domain Users
          AD_DOMAIN\dom_usr1
          CIFS_SERVER\engineering CIFS_SERVER\james
```

**Deleting a local group**

You can delete a local group from the Storage Virtual Machine (SVM) if it is no longer needed for determining access rights to data associated with that SVM or if it is no longer needed for assigning SVM user rights (privileges) to group members.

**About this task**

Keep the following in mind when deleting local groups:

- The file system is not altered.
  - Windows Security Descriptors on files and directories that refer to this group are not adjusted.
If the group does not exist, an error is returned.
The special Everyone group cannot be deleted.
Built-in groups such as BUILTIN\Administrators BUILTIN\Users cannot be deleted.

Steps
1. Determine the name of the local group that you want to delete by displaying the list of local groups on the SVM:

   vserver cifs users-and-groups local-group show -vserver vserver_name

2. Delete the local group:

   vserver cifs users-and-groups local-group delete -vserver vserver_name -group-name group_name

3. Verify that the group is deleted:

   vserver cifs users-and-groups local-user show -vserver vserver_name

Example

The following example deletes the local group “CIFS_SERVER\sales” associated with SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Svserver  Group Name                   Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1 -group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Svserver  Group Name                   Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering

vs1       CIFS_SERVER\sales
```

Updating domain user and group names in local databases

You can add domain users and groups to a CIFS server's local groups. These domain objects are registered in local databases on the cluster. If a domain object is renamed, the local databases must be manually updated.

About this task

You must specify the name of the Storage Virtual Machine (SVM) on which you want to update domain names.

Steps

1. Set the privilege level to advanced:

   set -privilege advanced

2. Perform the appropriate action:
If you want to update domain users and groups and...

Use this command...

| Display domain users and groups that successfully updated and that failed to update | `vserver cifs users-and-groups update-names -vserver vserver_name` |
| Display domain users and groups that successfully updated | `vserver cifs users-and-groups update-names -vserver vserver_name -display-failed-only false` |
| Display only the domain users and groups that fail to update | `vserver cifs users-and-groups update-names -vserver vserver_name -display-failed-only true` |
| Suppress all status information about updates | `vserver cifs users-and-groups update-names -vserver vserver_name -suppress-all-output true` |

3. Return to the admin privilege level:

`set -privilege admin`

Example

The following example updates the names of domain users and groups associated with Storage Virtual Machine (SVM, formerly known as Vserver) vs1. For the last update, there is a dependent chain of names that needs to be updated:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y
cluster1::*> vserver cifs users-and-groups update-names -vserver vs1
  Vserver:           vs1
  SID:               S-1-5-21-123456789-234565432-987654321-123456
  Domain:            EXAMPLE1
  Out-of-date Name:  dom_user1
  Updated Name:      dom_user2
  Status:            Successfully updated

  Vserver:           vs1
  SID:               S-1-5-21-123456789-234565432-987654322-23456
  Domain:            EXAMPLE2
  Out-of-date Name:  dom_user1
  Updated Name:      dom_user2
  Status:            Successfully updated

  Vserver:           vs1
  SID:               S-1-5-21-123456789-234565432-987654321-123456
  Domain:            EXAMPLE1
  Out-of-date Name:  dom_user3
  Updated Name:      dom_user4
  Status:            Successfully updated; also updated SID
  "S-1-5-21-123456789-234565432-987654321-123457" to name "dom_user5"; also updated SID
  "S-1-5-21-123456789-234565432-987654321-123458" to name "dom_user6"; also updated SID
  "S-1-5-21-123456789-234565432-987654321-123459" to name "dom_user7"; also updated SID
  "S-1-5-21-123456789-234565432-987654321-123460" to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been updated.
cluster1::*> set -privilege admin
```
Managing local privileges

You can manage local privileges by adding, removing, or resetting privileges for local and domain user accounts and groups. You can also display information about privileges assigned to local and domain user accounts and groups.

Related concepts

- How to assign privileges on page 217
- Managing local user accounts on page 221
- Managing local groups on page 227

Related references

- List of supported privileges on page 216

Adding privileges to local or domain users or groups

You can manage user rights for local or domain users or groups by adding privileges. The added privileges override the default privileges assigned to any of these objects. This provides enhanced security by allowing you to customize what privileges a user or group has.

Before you begin

The local or domain user or group to which privileges will be added must already exist.

About this task

Adding a privilege to an object overrides the default privileges for that user or group. Adding a privilege does not remove previously added privileges.

You must keep the following in mind when adding privileges to local or domain users or groups:

- You can add one or more privileges.
- When adding privileges to a domain user or group, Data ONTAP might validate the domain user or group by contacting the domain controller.

Steps

1. Add one or more privileges to a local or domain user or group:

   \`\`vserver cifs users-and-groups privilege add-privilege -vserver vserver\_name -user-or-group-name name -privileges privilege[,...]\`

   The value for the `-user-or-group-name` parameter is a local user or group, or a domain user or group.

   `-privileges privilege[,...]` is a comma-delimited list of one or more privileges.

2. Verify that the desired privileges are applied to the object:

   `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Example

The following example adds the privileges “SeTcbPrivilege” and “SeTakeOwnershipPrivilege” to the user “CIFS_SERVER\_sue” on Storage Virtual Machine (SVM, formerly known as Vserver) vs1:
Removing privileges from local or domain users or groups

You can manage user rights for local or domain users or groups by removing privileges. This provides enhanced security by allowing you to customize the maximum privileges that users and groups have.

Before you begin

The local or domain user or group from which privileges will be removed must already exist.

About this task

You must keep the following in mind when removing privileges from local or domain users or groups:

- You can remove one or more privileges.
- When removing privileges from a domain user or group, Data ONTAP might validate the domain user or group by contacting the domain controller. The command might fail if Data ONTAP is unable to contact the domain controller.

Steps

1. Remove one or more privileges from a local or domain user or group:

   ```bash
   vserver cifs users-and-groups privilege remove-privilege -vserver vserver_name -user-or-group-name name -privileges privilege[,...]
   ```

   The value for the `-user-or-group-name` parameter is a local user or group or a domain user or group.

   `-privileges privilege[,...]` is a comma-delimited list of one or more privileges.

2. Verify that the desired privileges have been removed from the object:

   ```bash
   vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name
   ```

Example

The following example removes the privileges “SeTcbPrivilege” and “SeTakeOwnershipPrivilege” from the user “CIFS_SERVER\sue” on Storage Virtual Machine (SVM, formerly known as Vserver) `vs1`:

```bash
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
          CIFS_SERVER\sue       SeTakeOwnershipPrivilege
```
Resetting privileges for local or domain users and groups

You can reset privileges for local or domain users and groups. This can be useful when you have made modifications to privileges for a local or domain user or group and those modifications are no longer wanted or needed.

About this task

Resetting privileges for a local or domain user or group removes any privilege entries for that object.

Steps

1. Reset the privileges on a local or domain user or group:

   ```bash
   vserver cifs users-and-groups privilege reset-privilege -vserver vserver_name -user-or-group-name name
   ```

   The value for the `-user-or-group-name` parameter is a local or domain user or group.

2. Verify that the privileges are reset on the object:

   ```bash
   vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name
   ```

Examples

The following example resets the privileges on the user “CIFS_SERVER\sue” on Storage Virtual Machine (SVM, formerly known as Vserver) vs1. By default, normal users do not have privileges associated with their accounts:

```
classcluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vaerven User or Group Name Priveleges
--------- --------------------- ---------------
vs1 CIFS_SERVER\sue SeTcbPrivilege
     SeTakeOwnershipPrivilege
```

```
classcluster1::> vserver cifs users-and-groups privilege reset-privilege -vserver vs1 -user-or-group-name CIFS_SERVER\sue
```

```
classcluster1::> vserver cifs users-and-groups privilege show -vserver vs1 -user-or-group-name CIFS_SERVER\sue
This table is currently empty.
```

The following example resets the privileges for the group “BUILTIN\Administrators”, effectively removing the privilege entry:

```
classcluster1::> vserver cifs users-and-groups privilege show -vserver vs1 -user-or-group-name BUILTIN\Administrators
Vaerven User or Group Name Priveleges
--------- --------------------- ---------------
vs1 BUILTIN\Administrators SeTcbPrivilege
     SeSecurityPrivilege
     SeTakeOwnershipPrivilege
```

```
classcluster1::> vserver cifs users-and-groups privilege reset-privilege -vserver vs1 -user-or-group-name BUILTIN\Administrators
```

```
classcluster1::> vserver cifs users-and-groups privilege show -vserver vs1 -user-or-group-name BUILTIN\Administrators
This table is currently empty.
```
Displaying information about privilege overrides

You can display information about custom privileges assigned to domain or local user accounts or groups. This information helps you determine whether the desired user rights are applied.

Step

1. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want to display information about...</th>
<th>Enter this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom privileges for all domain and local users and groups on the Storage Virtual Machine (SVM)</td>
<td><code>vserver cifs users-and-groups privilege show -vserver vserver_name</code></td>
</tr>
<tr>
<td>Custom privileges for a specific domain or local user and group on the SVM</td>
<td><code>vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name</code></td>
</tr>
</tbody>
</table>

There are other optional parameters that you can choose when you run this command. See the man page for more information.

Example

The following command displays all privileges explicitly associated with local or domain users and groups for SVM vs1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1

<table>
<thead>
<tr>
<th>Vserver</th>
<th>User or Group Name</th>
<th>Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>BUILTIN\Administrators</td>
<td>SeTakeOwnershipPrivilege</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SeRestorePrivilege</td>
</tr>
<tr>
<td>vs1</td>
<td>CIFS_SERVER\sue</td>
<td>SeTcbPrivilege</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SeTakeOwnershipPrivilege</td>
</tr>
</tbody>
</table>
```

Configuring bypass traverse checking

Bypass traverse checking is a user right (also known as a privilege) that determines whether a user can traverse all the directories in the path to a file even if the user does not have permissions on the traversed directory. You should understand what happens when allowing or disallowing bypass traverse checking, and how to configure bypass traverse checking for users on Storage Virtual Machines (SVMs).

What happens when allowing or disallowing bypass traverse checking

- If allowed, when a user attempts to access a file, Data ONTAP does not check the traverse permission for the intermediate directories when determining whether to grant or deny access to the file.
- If disallowed, Data ONTAP checks the traverse (execute) permission for all directories in the path to the file.
  If any of the intermediate directories do not have the “X” (traverse permission), Data ONTAP denies access to the file.
How to configure bypass traverse checking

You can configure bypass traverse checking by using the Data ONTAP CLI or by configuring Active Directory group policies with this user right.

The **SeChangeNotifyPrivilege** privilege controls whether users are allowed to bypass traverse checking.

- Adding it to local SMB users or groups on the SVM or to domain users or groups allows bypass traverse checking.
- Removing it from local SMB users or groups on the SVM or from domain users or groups disallows bypass traverse checking.

By default, the following BUILTIN groups on the SVM have the right to bypass traverse checking:

- BUILTIN\Administrators
- BUILTIN\Power Users
- BUILTIN\Backup Operators
- BUILTIN\Users
- Everyone

If you do not want to allow members of one of these groups to bypass traverse checking, you must remove this privilege from the group.

You must keep the following in mind when configuring bypass traverse checking for local SMB users and groups on the SVM by using the CLI:

- If you want to allow members of a custom local or domain group to bypass traverse checking, you must add the **SeChangeNotifyPrivilege** privilege to that group.
- If you want to allow an individual local or domain user to bypass traverse checking and that user is not a member of a group with that privilege, you can add the **SeChangeNotifyPrivilege** privilege to that user account.
- You can disable bypass traverse checking for local or domain users or groups by removing the **SeChangeNotifyPrivilege** privilege at any time.

**Note:** To disable bypass traverse checking for specified local or domain users or groups, you must also remove the **SeChangeNotifyPrivilege** privilege from the **Everyone** group.

**Related concepts**

- Securing file access by using SMB share ACLs on page 187
- Securing file access by using file permissions on page 190
- Managing local privileges on page 234

**Related tasks**

- Allowing users or groups to bypass directory traverse checking on page 239
- Disallowing users or groups from bypassing directory traverse checking on page 240
- Configuring character mapping for SMB file name translation on FlexVol volumes on page 161
- Creating an SMB share on a CIFS server on page 177

**Related references**

- List of supported privileges on page 216
Allowing users or groups to bypass directory traverse checking

If you want a user to be able traverse all the directories in the path to a file even if the user does not have permissions on a traversed directory, you can add the `SeChangeNotifyPrivilege` privilege to local SMB users or groups on Storage Virtual Machines (SVMs). By default, users are able to bypass directory traverse checking.

Before you begin

- A CIFS server must be exist on the SVM.
- The local users and groups CIFS server option must be enabled.
- The local or domain user or group to which the `SeChangeNotifyPrivilege` privilege will be added must already exist.

About this task

When adding privileges to a domain user or group, Data ONTAP might validate the domain user or group by contacting the domain controller. The command might fail if Data ONTAP cannot contact the domain controller.

Steps

1. Enable bypass traverse checking by adding the `SeChangeNotifyPrivilege` privilege to a local or domain user or group:
   ```bash
   vserver cifs users-and-groups privilege add-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege
   ```
   The value for the `-user-or-group-name` parameter is a local user or group, or a domain user or group.

2. Verify that the specified user or group has bypass traverse checking enabled:
   ```bash
   vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name
   ```

Example

The following command enables users that belong to the “EXAMPLE\eng” group to bypass directory traverse checking by adding the `SeChangeNotifyPrivilege` privilege to the group:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver     User or Group Name     Privileges
------------ ------------------------ ------------------------
vs1          EXAMPLE\eng            SeChangeNotifyPrivilege
```

Related tasks

- [Disallowing users or groups from bypassing directory traverse checking](#) on page 240
Disallowing users or groups from bypassing directory traverse checking

If you do not want a user to traverse all the directories in the path to a file because the user does not have permissions on the traversed directory, you can remove the SeChangeNotifyPrivilege privilege from local SMB users or groups on Storage Virtual Machines (SVMs).

Before you begin

The local or domain user or group from which privileges will be removed must already exist.

About this task

When removing privileges from a domain user or group, Data ONTAP might validate the domain user or group by contacting the domain controller. The command might fail if Data ONTAP cannot contact the domain controller.

Steps

1. Disallow bypass traverse checking:

   ```bash
   vserver cifs users-and-groups privilege remove-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege
   ```

   The command removes the SeChangeNotifyPrivilege privilege from the local or domain user or group that you specify with the value for the -user-or-group-name name parameter.

2. Verify that the specified user or group has bypass traverse checking disabled:

   ```bash
   vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name
   ```

Example

The following command disallows users that belong to the “EXAMPLE\eng” group from bypassing directory traverse checking:

```bash
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver  User or Group Name  Privileges
--------- --------------------- -----------------------
vs1      EXAMPLE\eng         SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege -vserver vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver  User or Group Name  Privileges
--------- --------------------- -----------------------
vs1      EXAMPLE\eng         -
```

Related tasks

- **Allowing users or groups to bypass directory traverse checking** on page 239

Displaying information about file security and audit policies

You can display information about file security on files and directories contained within volumes on Storage Virtual Machines (SVMs). You can display information about audit policies on FlexVol
If configured, you can display information about Storage-Level Access Guard and Dynamic Access Control security settings on FlexVol volumes.

**Displaying information about file security**
You can display information about file security applied to data contained within volumes and qtrees (for FlexVol volumes) with the following security styles:

- NTFS
- UNIX
- Mixed
- Unified (for Infinite Volume)

**Displaying information about audit policies**
You can display information about audit policies for auditing access events on FlexVol volumes over the following NAS protocols:

- SMB (all versions)
- NFSv4.x

*Note:* Although it is possible to configure SACLs on files and directories contained within an Infinite Volume, clustered Data ONTAP does not support auditing on SVMs with Infinite Volume.

**Displaying information about Storage-Level Access Guard (SLAG) security**
Storage-Level Access Guard security can be applied on FlexVol volumes objects with the following security styles:

- NTFS
- Mixed
- UNIX (if a CIFS server is configured on the SVM that contains the volume)

**Displaying information about Dynamic Access Control (DAC) security**
Dynamic Access Control security can be applied on an object within a FlexVol volume with the following security styles:

- NTFS
- Mixed (if the object has NTFS effective security)

**Related concepts**

- *How security styles affect data access* on page 20
- *Managing NTFS file security, NTFS audit policies, and Storage-Level Access Guard on SVMs using the CLI* on page 251
- *Securing file access by using Storage-Level Access Guard* on page 152

**Related tasks**

- *Displaying information about Storage-Level Access Guard* on page 158
- *Performing security traces* on page 285
Displaying information about file security on NTFS security-style volumes

You can display information about file and directory security on NTFS security-style volumes, including what the security style and effective security styles are, what permissions are applied, and information about DOS attributes. You can use the results to validate your security configuration or to troubleshoot file access issues.

About this task

You must supply the name of the Storage Virtual Machine (SVM) and the path to the data whose file or folder security information you want to display. You can display the output in summary form or as a detailed list.

• Because NTFS security-style volumes and qtrees use only NTFS file permissions and Windows users and groups when determining file access rights, UNIX-related output fields contain display-only UNIX file permission information.

• ACL output is displayed for file and folders with NTFS security.

• Because Storage-Level Access Guard security can be configured on the volume root or qtree, output for a volume or qtree path where Storage-Level Access Guard is configured might display both regular file ACLs and Storage-Level Access Guard ACLs.

• The output also displays information about Dynamic Access Control ACEs if Dynamic Access Control is configured for the given file or directory path.

Step

1. Display file and directory security settings with the desired level of detail:

<table>
<thead>
<tr>
<th>If you want to display information...</th>
<th>Enter the following command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>In summary form</td>
<td><code>vserver security file-directory show -vserver vserver_name -path path</code></td>
</tr>
<tr>
<td>With expanded detail</td>
<td><code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code></td>
</tr>
</tbody>
</table>

Examples

The following example displays the security information about the path `/vol4` in SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4
Vserver: vs1
File Path: /vol4
File Inode Number: 64
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
Unix User Id: 0
Unix Group Id: 0
Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
  Control:0x8004
  Owner: BUILTIN\Administrators
  Group: BUILTIN\Administrators
  DACL - ACEs
    ALLOW-Everyone-0x1f01ff
    ALLOW-Everyone-0x10000000-OI|CI|IO
```

The following example displays the security information with expanded masks about the path `/data/engineering` in SVM vs1:
The following example displays security information, including Storage-Level Access Guard security information, for the volume with the path /data/vol1 in SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path /data/engineering -expand-mask true

Vserver: vs1
File Path: /data/engineering
File Inode Number: 5544
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
Expanded Dos Attributes: 0x10
...0 ...... ...... = Offline
...0 ...... ...... = Sparse
...0 ...... ...... = Normal
...0 ...... ...... = Archive
...1 ...... ...... = Directory
...0 ...... ...... = System
...0 ...... ...... = Hidden
0 ...... ...... = Read Only
Unix User Id: 0
Unix Group Id: 0
Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
Control:0x8004

1... ...... ...... = Self Relative
.0. ...... ...... = RM Control Valid
.0. ...... ...... = SACL Protected
...0 ...... ...... = DACL Protected
...... 00...... = SACL Inherited
...... 00...... = DACL Inherited
...... 00...... = SACL Inherit Required
...... 00...... = DACL Inherit Required
...... 0...... = SACL Defaulted
...... 0...... = DACL Defaulted
...... 0...... = Group Defaulted
...... 0...... = Owner Defaulted

Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
DACL - ACEs
ALLOW-Everyone-0x1f00ff
0... ...... ...... ...... ...... ...... ...... ...... = Generic Read
.0. ...... ...... ...... ...... ...... ...... ...... = Generic Write
.0. ...... ...... ...... ...... ...... ...... ...... = Generic Execute
.0. ...... ...... ...... ...... ...... ...... ...... = Generic All
...... 00...... = SACL Inherited
...... 00...... = DACL Inherited
...... 00...... = SACL Inherit Required
...... 00...... = DACL Inherit Required
...... 0...... = SACL Defaulted
...... 0...... = DACL Defaulted
...... 0...... = Group Defaulted
...... 0...... = Owner Defaulted

ALLOW-Everyone-0x10000000-01|CI|ID
0... ...... ...... ...... ...... ...... ...... ...... = Generic Read
.0. ...... ...... ...... ...... ...... ...... ...... = Generic Write
.0. ...... ...... ...... ...... ...... ...... ...... = Generic Execute
.0. ...... ...... ...... ...... ...... ...... ...... = Generic All
...... 00...... = SACL Inherited
...... 00...... = DACL Inherited
...... 00...... = SACL Inherit Required
...... 00...... = DACL Inherit Required
...... 0...... = SACL Defaulted
...... 0...... = DACL Defaulted
...... 0...... = Group Defaulted
...... 0...... = Owner Defaulted

The following example displays security information, including Storage-Level Access Guard security information, for the volume with the path /data/vol1 in SVM vs1:
```
cluster::> vserver security file-directory show -vserver vs1 -path /datavol1

Vserver: vs1
File Path: /datavol1
File Inode Number: 77
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
Unix User Id: 0
Unix Group Id: 0
Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
Control:0x8004
Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
DACL - ACEs
ALLOW-Everyone-0x1f01ff
ALLOW-Everyone-0x10000000-OI|CI|IO

Storage-Level Access Guard security
SACL (Applies to Directories):
AUDIT-EXAMPLE\Domain Users-0x120089-FA
AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Directories):
ALLOW-EXAMPLE\Domain Users-0x120089
ALLOW-EXAMPLE\engineering-0x1f01ff
ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
SACL (Applies to Files):
AUDIT-EXAMPLE\Domain Users-0x120089-FA
AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Files):
ALLOW-EXAMPLE\Domain Users-0x120089
ALLOW-EXAMPLE\engineering-0x1f01ff
ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

Related tasks
Displaying information about file security on mixed security-style volumes on page 244
Displaying information about file security on UNIX security-style volumes on page 246

Related information
Clustered Data ONTAP 8.3.1 man page: vserver security file-directory show - Display file/folder security information

Displaying information about file security on mixed security-style volumes

You can display information about file and directory security on mixed security-style volumes, including what the security style and effective security styles are, what permissions are applied, and information about UNIX owners and groups. You can use the results to validate your security configuration or to troubleshoot file access issues.

About this task
You must supply the name of the Storage Virtual Machine (SVM) and the path to the data whose file or folder security information you want to display. You can display the output in summary form or as a detailed list.

- Mixed security-style volumes and qtrees can contain some files and folders that use UNIX file permissions, either mode bits or NFSv4 ACLs, and some files and directories that use NTFS file permissions.
- The top level of a mixed security-style volume can have either UNIX or NTFS effective security.
- ACL output is displayed only for file and folders with NTFS or NFSv4 security. This field is empty for files and directories using UNIX security that have only mode bit permissions applied (no NFSv4 ACLs).
The owner and group output fields in the ACL output apply only in the case of NTFS security descriptors.

Because Storage-Level Access Guard security can be configured on a mixed security-style volume or qtree even if the effective security style of the volume root or qtree is UNIX, output for a volume or qtree path where Storage-Level Access Guard is configured might display both UNIX file permissions and Storage-Level Access Guard ACLs.

If the path entered in the command is to data with NTFS effective security, the output also displays information about Dynamic Access Control ACEs if Dynamic Access Control is configured for the given file or directory path.

### Step

1. Display file and directory security settings with the desired level of detail:

<table>
<thead>
<tr>
<th>If you want to display information...</th>
<th>Enter the following command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>In summary form</td>
<td>vserver security file-directory show -vserver vserver_name -path path</td>
</tr>
<tr>
<td>With expanded detail</td>
<td>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</td>
</tr>
</tbody>
</table>

### Examples

The following example displays the security information about the path `/projects` in SVM vs1 in expanded-mask form. This mixed security-style path has UNIX effective security.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /projects -expand-mask true

Vserver: vs1
File Path: /projects
File Inode Number: 78
Security Style: mixed
Effective Style: unix
DOS Attributes: 10
DOS Attributes in Text: -----D---
Expanded Dos Attributes: 0x10
    ...0    = Offline
    ...0    = Sparse
    ...0    = Normal
    ...1    = Archive
    ...1    = Directory
    ....    = System
    ....    = Hidden
    ....    = Read Only
Unix User Id: 0
Unix Group Id: 1
 Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx------
ACLs: -
```

The following example displays the security information about the path `/data` in SVM vs1. This mixed security-style path has an NTFS effective security.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data

Vserver: vs1
File Path: /data
File Inode Number: 544
Security Style: mixed
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: -----D---
Expanded Dos Attributes: -
    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
```
The following example displays the security information about the volume at the path /datavol5 in SVM vs1. The top level of this mixed security-style volume has UNIX effective security. The volume has Storage-Level Access Guard security.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /datavol5
```

Vserver: vs1
File Path: /datavol5
File Inode Number: 3374
Security Style: mixed
Effective Style: unix
DOS Attributes: 10
DOS Attributes in Text: ----D---
Unix User Id: 0
Unix Group Id: 0
Unix Mode Bits: 755
Unix Mode Bits in Text: rwxr-xr-x
ACLs: Storage-Level Access Guard security
SACL (Applies to Directories):
  AUDIT-EXAMPLE\Domain Users-0x120089-FA
  AUDIT-EXAMPLE\engineering-0x1f01ff-SA
  AUDIT-EXAMPLE\market-0x1f01ff-SA
DACL (Applies to Directories):
  ALLOW-BUILTIN\Administrators-0x1f01ff
  ALLOW-CREATOR OWNER-0x1f01ff
  ALLOW-EXAMPLE\Domain Users-0x120089
  ALLOW-EXAMPLE\engineering-0x1f01ff
  ALLOW-EXAMPLE\market-0x1f01ff
SACL (Applies to Files):
  AUDIT-EXAMPLE\Domain Users-0x120089-FA
  AUDIT-EXAMPLE\engineering-0x1f01ff-SA
  AUDIT-EXAMPLE\market-0x1f01ff-SA
DACL (Applies to Files):
  ALLOW-BUILTIN\Administrators-0x1f01ff
  ALLOW-CREATOR OWNER-0x1f01ff
  ALLOW-EXAMPLE\Domain Users-0x120089
  ALLOW-EXAMPLE\engineering-0x1f01ff
  ALLOW-EXAMPLE\market-0x1f01ff

Related tasks

- Displaying information about file security on NTFS security-style volumes on page 242
- Displaying information about file security on UNIX security-style volumes on page 246

Related information

- Clustered Data ONTAP 8.3.1 man page: vserver security file-directory show - Display file/folder security information

Displaying information about file security on UNIX security-style volumes

You can display information about file and directory security on UNIX security-style volumes, including what the security styles and effective security styles are, what permissions are applied, and information about UNIX owners and groups. You can use the results to validate your security configuration or to troubleshoot file access issues.

About this task

You must supply the name of the Storage Virtual Machine (SVM) and the path to the data whose file or directory security information you want to display. You can display the output in summary form or as a detailed list.

- UNIX security-style volumes and qtrees use only UNIX file permissions, either mode bits or NFSv4 ACLs when determining file access rights.
• ACL output is displayed only for file and folders with NFSv4 security. This field is empty for files and directories using UNIX security that have only mode bit permissions applied (no NFSv4 ACLs).

• The owner and group output fields in the ACL output does not apply in the case of NFSv4 security descriptors. They are only meaningful for NTFS security descriptors.

• Because Storage-Level Access Guard security is supported on a UNIX volume or qtree if a CIFS server is configured on the SVM, the output might contain information about Storage-Level Access Guard security applied to the volume or qtree specified in the `-path` parameter.

**Step**

1. Display file and directory security settings with the desired level of detail:

<table>
<thead>
<tr>
<th>If you want to display information...</th>
<th>Enter the following command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>In summary form</td>
<td><code>vserver security file-directory show -vserver vserver_name -path path</code></td>
</tr>
<tr>
<td>With expanded detail</td>
<td><code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code></td>
</tr>
</tbody>
</table>

**Examples**

The following example displays the security information about the path `/home` in SVM vs1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home

Vserver: vs1
File Path: /home
File Inode Number: 9590
Security Style: unix
Effective Style: unix
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
Unix User Id: 0
Unix Group Id: 1
Unix Mode Bits: 700
Unix Mode Bits in Text: rwx------
ACLs: -
```

The following example displays the security information about the path `/home` in SVM vs1 in expanded-mask form:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home -expand-mask true

Vserver: vs1
File Path: /home
File Inode Number: 9590
Security Style: unix
Effective Style: unix
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
...0 .... ..... = Offline
..... ...0 ...... = Sparse
..... 0... .... = Normal
..... ..... .0. = Archive
..... ..... 1.... = Directory
..... ..... ...1. = System
..... ..... ..... = Hidden
..... ..... ..... = Read Only
Unix User Id: 0
Unix Group Id: 1
Unix Mode Bits: 700
Unix Mode Bits in Text: rwx------
ACLs: -
```
Displaying information about NTFS audit policies on FlexVol volumes using the CLI

You can display information about NTFS audit policies on FlexVol volumes, including what the security styles and effective security styles are, what permissions are applied, and information about system access control lists. You can use the results to validate your security configuration or to troubleshoot auditing issues.

About this task

You must supply the name of the Storage Virtual Machine (SVM) and the path to the files or folders whose audit information you want to display. You can display the output in summary form or as a detailed list.

1. NTFS security-style volumes and qtrees use only NTFS SACLs (system access control lists) for audit policies.
2. Files and folders in a mixed security-style volume with NTFS effective security can have NTFS audit policies applied to them.
3. Mixed security-style volumes and qtrees can contain some files and directories that use UNIX file permissions, either mode bits or NFSv4 ACLs, and some files and directories that use NTFS file permissions.
4. The top level of a mixed security-style volume can have either UNIX or NTFS effective security and might or might not contain NTFS SACLs.
5. Because Storage-Level Access Guard security can be configured on a mixed security-style volume or qtree even if the effective security style of the volume root or qtree is UNIX, output for a volume or qtree path where Storage-Level Access Guard is configured might display both regular file and folder NFSv4 SACLs and Storage-Level Access Guard NTFS SACLs.
6. If the path entered in the command is to data with NTFS effective security, the output also displays information about Dynamic Access Control ACEs if Dynamic Access Control is configured for the given file or directory path.
7. When displaying security information about files and folders with NTFS effective security, UNIX-related output fields contain display-only UNIX file permission information. NTFS security-style files and folders use only NTFS file permissions and Windows users and groups when determining file access rights.
8. ACL output is displayed only for file and folders with NTFS or NFSv4 security. This field is empty for files and folders using UNIX security that have only mode bit permissions applied (no NFSv4 ACLs).
9. The owner and group output fields in the ACL output apply only in the case of NTFS security descriptors.

Step

1. Display file and directory audit policy settings with the desired level of detail:
If you want to display information...

Enter the following command...

<table>
<thead>
<tr>
<th>In summary form</th>
<th>vserver security file-directory show -vserver vserver_name -path path</th>
</tr>
</thead>
<tbody>
<tr>
<td>With expanded detail</td>
<td>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</td>
</tr>
</tbody>
</table>

### Examples

The following example displays the audit policy information about the path /corp in SVM vs1. The path has NTFS effective security. The NTFS security descriptor contains both a SUCCESS and a SUCCESS/FAIL SACL entry.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
Vserver: vs1
File Path: /corp
File Inode Number: 357
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
Unix User Id: 0
Unix Group Id: 0
Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
Control:0x8014
Owner:DOMAIN\Administrator
Group:BUILTIN\Administrators
SACL - ACEs
ALL-DOMAIN\Administrator-0x100081-0|CI|SA|FA
SUCCESSFUL-DOMAIN\user1-0x100116-0|CI|SA
DACL - ACEs
ALLOW-BUILTIN\Administrators-0x1f01ff-0|CI
ALLOW-BUILTIN\Users-0x1f01ff-0|CI
ALLOW-CREATOR OWNER-0x1f01ff-0|CI
ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-0|CI
```

The following example displays the audit policy information about the path /datavol1 in SVM vs1. The path contains both regular file and folder SACLs and Storage-Level Access Guard SACLs.

```
cluster::> vserver security file-directory show -vserver vs1 -path /datavol1
Vserver: vs1
File Path: /datavol1
File Inode Number: 77
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
Unix User Id: 0
Unix Group Id: 0
Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
Control:0xaa14
Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
SACL - ACEs
AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
DACL - ACEs
ALLOW-EXAMPLE\Domain Admins-0x1f01ff-0|CI
ALLOW-EXAMPLE\marketing-0x1200a9-0|CI
Storage-Level Access Guard security
SACL (Applies to Directories):
AUDIT-EXAMPLE\Domain Users-0x120089-FA
AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Directories):
ALLOW-EXAMPLE\Domain Users-0x120089
ALLOW-EXAMPLE\engineering-0x1f01ff
ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
SACL (Applies to Files):
AUDIT-EXAMPLE\Domain Users-0x120089-FA
AUDIT-EXAMPLE\engineering-0x1f01ff-SA
```
Displaying information about NFSv4 audit policies on FlexVol volumes using the CLI

You can display information about NFSv4 audit policies on FlexVol volumes using the Data ONTAP CLI, including what the security styles and effective security styles are, what permissions are applied, and information about system access control lists (SACLs). You can use the results to validate your security configuration or to troubleshoot auditing issues.

About this task

You must supply the name of the Storage Virtual Machine (SVM) and the path to the files or directories whose audit information you want to display. You can display the output in summary form or as a detailed list.

• UNIX security-style volumes and qtrees use only NFSv4 SACLs for audit policies.
• Files and directories in a mixed security-style volume that are of UNIX security style can have NFSv4 audit policies applied to them.
• Mixed security-style volumes and qtrees can contain some files and directories that use UNIX file permissions, either mode bits or NFSv4 ACLs, and some files and directories that use NTFS file permissions.
• The top level of a mixed security-style volume can have either UNIX or NTFS effective security and might or might not contain NFSv4 SACLs.
• ACL output is displayed only for file and folders with NTFS or NFSv4 security. This field is empty for files and folders using UNIX security that have only mode bit permissions applied (no NFSv4 ACLs).
• The owner and group output fields in the ACL output apply only in the case of NTFS security descriptors.
• Because Storage-Level Access Guard security can be configured on a mixed security-style volume or qtree even if the effective security style of the volume root or qtree is UNIX, output for a volume or qtree path where Storage-Level Access Guard is configured might display both regular NFSv4 file and directory SACLs and Storage-Level Access Guard NTFS SACLs.
• Because Storage-Level Access Guard security is supported on a UNIX volume or qtree if a CIFS server is configured on the SVM, the output might contain information about Storage-Level Access Guard security applied to the volume or qtree specified in the -path parameter.

Step

1. Display file and directory security settings with the desired level of detail:

<table>
<thead>
<tr>
<th>If you want to display information...</th>
<th>Enter the following command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>In summary form</td>
<td>vserver security file-directory show -vserver vserver_name -path path</td>
</tr>
<tr>
<td>With expanded detail</td>
<td>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</td>
</tr>
</tbody>
</table>
Managing NTFS file security, NTFS audit policies, and Storage-Level Access Guard on SVMs using the CLI

You can manage NTFS file security, NTFS audit policies, and Storage-Level Access Guard on Storage Virtual Machines (SVMs) with FlexVol volumes by using the CLI.

You can manage NTFS file security and audit policies from SMB clients or by using the CLI. However, using the CLI to configure file security and audit policies removes the need to use a remote client to manage file security. Using the CLI can significantly reduce the time it takes to apply security on many files and folders using a single command.

You can configure Storage-Level Access Guard, which is another layer of security applied by Data ONTAP to SVM volumes. Storage-Level Access Guard applies to accesses from all NAS protocols to the storage object to which Storage-Level Access Guard is applied.

Storage-Level Access Guard can be configured and managed only from the Data ONTAP CLI. You cannot manage Storage-Level Access Guard settings from SMB clients. Moreover, if you view the security settings on a file or directory from an NFS or SMB client, you will not see the Storage-Level Access Guard security. Storage-Level Access Guard security cannot be revoked from a client, even by a system (Windows or UNIX) administrator. Therefore, Storage-Level Access Guard provides an extra layer of security for data access that is independently set and managed by the storage administrator.

**Note:** Even though only NTFS access permissions are supported for Storage-Level Access Guard, Data ONTAP can perform security checks for access over NFS to data on volumes where Storage-Level Access Guard is applied if the UNIX user maps to a Windows user on the SVM that owns the volume.

**NTFS security-style volumes**

All files and folders contained within NTFS security-style volumes and qtrees have NTFS effective security. You can use the `vserver security file-directory` command family to implement the following types of security on NTFS security-style volumes:

- File permissions and audit policies to files and folders contained in the volume
- Storage-Level Access Guard security on volumes
Mixed security-style volumes

Mixed security-style volumes and qtrees can contain some files and folders that have UNIX effective security and use UNIX file permissions, either mode bits or NFSv4.x ACLs and NFSv4.x audit policies, and some files and folders that have NTFS effective security and use NTFS file permissions and audit policies. You can use the `vserver security file-directory` command family to apply the following types of security to mixed security-style data:

- File permissions and audit policies to files and folders with NTFS effective security-style in the mixed volume or qtree
- Storage-Level Access Guard to volumes with either NTFS and UNIX effective security-style

UNIX security-style volumes

UNIX security-style volumes and qtrees contain files and folders that have UNIX effective security (either mode bits or NFSv4.x ACLs). You must keep the following in mind if you want to use the `vserver security file-directory` command family to implement security on UNIX security-style volumes:

- The `vserver security file-directory` command family cannot be used to manage UNIX file security and audit policies on UNIX security-style volumes and qtrees.
- You can use the `vserver security file-directory` command family to configure Storage-Level Access Guard on UNIX security-style volumes, provided the SVM with the target volume contains a CIFS server.

Related concepts

- Displaying information about file security and audit policies on page 240
- Securing file access by using Storage-Level Access Guard on page 152

Related tasks

- Configuring and applying file security on NTFS files and folders using the CLI on page 255
- Configuring and applying audit policies on NTFS files and folders using the CLI on page 268

Use cases for using the CLI to set file and folder security

Because you can apply and manage file and folder security locally without involvement from a remote client, you can significantly reduce the time it takes to set bulk security on a large number of files or folders.

You can benefit from using the CLI to set file and folder security in the following use cases:

- Storage of files in large enterprise environments, such as file storage in home directories
- Migration of data
- Change of Windows domain
- Standardization of file security and audit policies across NTFS file systems

Limits when using the CLI to set file and folder security

You need to be aware of certain limits when using the CLI to set file and folder security.

- The `vserver security file-directory` command family does not support setting NFSv4 ACLs.
- You can only apply NTFS security descriptors to NTFS files and folders.
The vserver security file-directory command family does not support setting file security (NTFS or NFSv4) on Storage Virtual Machines (SVMs) with Infinite Volume.

How security descriptors are used to apply file and folder security

Security descriptors contain the access control lists that determine what actions a user can perform on files and folders, and what is audited when a user accesses files and folders.

Permissions

Permissions are allowed or denied by an object’s owner and determine what actions an object (users, groups, or computer objects) can perform on specified files or folders.

Security descriptors

Security descriptors are data structures that contain security information that define permissions associated with a file or folder.

Access control lists (ACLs)

Access control lists are the lists contained within a security descriptor that contain information on what actions users, groups, or computer objects can perform on the file or folder to which the security descriptor is applied. The security descriptor can contain the following two types of ACLs:

- Discretionary access control lists (DACLs)
- System access control lists (SACLs)

Discretionary access control lists (DACLs)

DACLs contain the list of SIDS for the users, groups, and computer objects who are allowed or denied access to perform actions on files or folders. DACLs contain zero or more access control entries (ACEs).

System access control lists (SACLs)

SACLs contain the list of SIDS for the users, groups, and computer objects for which successful or failed auditing events are logged. SACLs contain zero or more access control entries (ACEs).

Access Control Entries (ACEs)

ACEs are individual entries in either DACLs or SACLs:

- A DACL access control entry specifies the access rights that are allowed or denied for particular users, groups, or computer objects.
- A SACL access control entry specifies the success or failure events to log when auditing specified actions performed by particular users, groups, or computer objects.

Permission inheritance

Permission inheritance describes how permissions defined in security descriptors are propagated to an object from a parent object. Only inheritable permissions are inherited by child objects. When setting permissions on the parent object, you can decide whether folders, sub-folders, and files can inherit them with “Apply to this-folder, sub-folders, and files”.

Related tasks

Configuring and applying file security on NTFS files and folders using the CLI on page 255
Configuring standard NTFS file permissions by using the Windows Security tab on page 190
Configuring advanced NTFS file permissions using the Windows Security tab on page 192
Configuring and applying audit policies on NTFS files and folders using the CLI on page 268
Configuring NTFS audit policies using the Windows Security tab on page 439
Considerations when applying file-directory policies that use local users or groups on the SVM disaster recovery destination

There are certain considerations that you must keep in mind before applying file-directory policies on the Storage Virtual Machine (SVM) disaster recovery destination in an ID discard configuration if your file-directory policy configuration uses local users or groups in either the security descriptor or the DACL or SACL entries.

You can configure a disaster recovery configuration for an SVM where the source SVM on the source cluster replicates the data and configuration from the source SVM to a destination SVM on a destination cluster.

You can set up one of two types of SVM disaster recovery.

- **Identity preserved**
  With this configuration, the identity of the SVM and the CIFS server is preserved.

- **Identity discarded**
  With this configuration, the identity of the SVM and the CIFS server is not preserved. In this scenario, the name of the SVM and the CIFS server on the destination SVM is different from the SVM and the CIFS server name on the source SVM.

Consideration for identity discarded configuration

In an identity discarded configuration, for an SVM source that contains local user, group, and privilege configurations, the name of the local domain (local CIFS server name) must be changed to match the CIFS server name on the SVM destination. For example, if the source SVM name is “vs1” and CIFS server name is “CIFS1” and the destination SVM name is “vs1_dst” and the CIFS server name is “CIFS1_DST”, the local domain name for a local user named “CIF1\user1” is automatically changed to “CIFS1_DST\user1” on the destination SVM:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst
Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- --------------
vs1          CIFS1\Administrator                     Built-in administrator account
vs1          CIFS1\user1              -              -
```

```
cluster1dst::> vserver cifs users-and-groups local-user show -vserver vs1_dst
Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- --------------
vs1_dst      CIFS1_DST\Administrator                 Built-in administrator account
vs1_dst      CIFS1_DST\user1          -              -
```

Even though local user and group names are automatically changed in the local user and group databases, local users or group names are not automatically changed in file-directory policy configurations (policies configured on the CLI using the `vserver security file-directory` command family).

For example, for “vs1”, if you have configured a DACL entry where the `-account` parameter is set to “CIFS\user1”, the setting will not be automatically changed on the destination SVM to reflect the destination's CIFS server name.

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1
Vserver: vs1
NTFS Security Descriptor Name: sd1
```
You must use the `vserver security file-directory modify` commands to manually change the CIFS server name to the destination CIFS server name.

**File-directory policy configuration components that contain account parameters**

There are three file-directory policy configuration components that can use parameter settings that can contain local users or groups:

- **Security descriptor**

  You can optionally specify the owner of the security descriptor and the primary group of the owner of the security descriptor. If the security descriptor uses a local user or group for the owner and primary group entries, you must modify the security descriptor to use the destination SVM in the account name. You can use the `vserver security file-directory ntfs modify` command to make any necessary changes to the account names.

- **DACL entries**

  Each DACL entry must be associated with an account. You must modify any DACLs that use local user or group accounts to use the destination SVM name. Because you cannot modify the account name for existing DACL entries, you must remove any DACL entries with local users or groups from the security descriptors, create new DACL entries with the corrected destination account names, and associate these new DACL entries with the appropriate security descriptors.

- **SACL entries**

  Each SACL entry must be associated with an account. You must modify any SACLs that use local user or group accounts to use the destination SVM name. Because you cannot modify the account name for existing SACL entries, you must remove any SACL entries with local users or groups from the security descriptors, create new SACL entries with the corrected destination account names, and associate these new SACL entries with the appropriate security descriptors.

You must make any necessary changes to local users or groups used in the file-directory policy configuration before applying the policy; otherwise, the apply job fails.

**Configuring and applying file security on NTFS files and folders using the CLI**

There are several steps you must perform to apply NTFS file security when using the Data ONTAP CLI. First, you create an NTFS security descriptor and add DACLs to the security descriptor. Next you create a security policy and add policy tasks. You then apply the security policy to a Storage Virtual Machine (SVM) with FlexVol volumes.

**About this task**

After applying the security policy, you can monitor the security policy job and then verify the settings on the applied file security.
Steps

1. **Creating an NTFS security descriptor** on page 257
   Creating an NTFS security descriptor is the first step in configuring and applying NTFS access control lists (ACLs) to files and folders residing within Storage Virtual Machines (SVMs) with FlexVol volumes. You will associate the security descriptor to the file or folder path in a policy task.

2. **Adding NTFS DACL access control entries to the NTFS security descriptor** on page 259
   Adding DACL (discretionary access control list) access control entries (ACEs) to the NTFS security descriptor is the second step in configuring and applying NTFS ACLs to a file or folder. Each entry identifies which object is allowed or denied access, and defines what the object can or cannot do to the files or folders defined in the ACE.

3. **Creating a security policy** on page 261
   Creating a security policy for Storage Virtual Machines (SVMs) with FlexVol volumes is the third step in configuring and applying ACLs to a file or folder. A policy acts as a container for various tasks where each task is a single entry that can be applied to files or folders. You later add tasks to the security policy.

4. **Adding a task to the security policy** on page 262
   Creating and adding a policy task to a security policy is the fourth step in configuring and applying ACLs to files or folders in Storage Virtual Machines (SVMs) with FlexVol volumes. When you create the policy task, you associate the task with a security policy. You can add one or more task entries to a security policy.

5. **Applying security policies** on page 265
   Applying a security policy to Storage Virtual Machines (SVMs) with FlexVol volumes is the last step to creating and applying NTFS ACLs to files or folders.

6. **Monitoring the security policy job** on page 266
   When applying the security policy to Storage Virtual Machines (SVMs) with FlexVol volumes, you can monitor the progress of the task by monitoring the security policy job. This is helpful if you want to ascertain that the application of the security policy succeeded. This is also helpful if you have a long-running job where you are applying bulk security to a large number of files and folders.

7. **Verifying the applied file security** on page 266
   You can verify the file security settings to confirm that the files or folders on the Storage Virtual Machine (SVM) with FlexVol volumes to which you applied the security policy have the desired settings.

Related concepts

- *Securing file access by using Storage-Level Access Guard* on page 152
- *Limits when using the CLI to set file and folder security* on page 252
- *How security descriptors are used to apply file and folder security* on page 253

Related tasks

- *Configuring standard NTFS file permissions by using the Windows Security tab* on page 190
- *Configuring advanced NTFS file permissions using the Windows Security tab* on page 192
- *Displaying information about file security on NTFS security-style volumes* on page 242
- *Displaying information about file security on mixed security-style volumes* on page 244
- *Displaying information about file security on UNIX security-style volumes* on page 246
- *Configuring and applying audit policies on NTFS files and folders using the CLI* on page 268
Creating an NTFS security descriptor

Creating an NTFS security descriptor is the first step in configuring and applying NTFS access control lists (ACLs) to files and folders residing within Storage Virtual Machines (SVMs) with FlexVol volumes. You will associate the security descriptor to the file or folder path in a policy task.

About this task

You can create NTFS security descriptors for files and folders residing within NTFS security-style volumes, or for files and folders residing on mixed security-style volumes.

By default, when a security descriptor is created, four discretionary access control list (DACL) access control entries (ACEs) are added to that security descriptor. The four default ACEs are as follows:

<table>
<thead>
<tr>
<th>Object</th>
<th>Access type</th>
<th>Access rights</th>
<th>Where to apply the permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>BUILTIN\Administrators</td>
<td>Allow</td>
<td>Full Control</td>
<td>this-folder, sub-folders, files</td>
</tr>
<tr>
<td>BUILTIN\Users</td>
<td>Allow</td>
<td>Full Control</td>
<td>this-folder, sub-folders, files</td>
</tr>
<tr>
<td>CREATOR OWNER</td>
<td>Allow</td>
<td>Full Control</td>
<td>this-folder, sub-folders, files</td>
</tr>
<tr>
<td>NT AUTHORITY \SYSTEM</td>
<td>Allow</td>
<td>Full Control</td>
<td>this-folder, sub-folders, files</td>
</tr>
</tbody>
</table>

When creating the security descriptor, you must specify the following two parameters:

<table>
<thead>
<tr>
<th>Required parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| -vserver vserver_name | SVM name  
The name of the SVM that contains the files and folders to which you want to apply the security descriptor. |
| -ntfs-sd SD_name | Security descriptor  
The name to assign to the security descriptor. |

You can customize the security descriptor configuration by using the following optional parameters:

<table>
<thead>
<tr>
<th>Optional parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| -owner name_or_SID | Owner of the security descriptor  
The owner of the security descriptor can modify the permissions on the files (or folders) to which the security descriptor is applied and can give other users the right to take ownership of the objects to which the security descriptor is applied. You can use any of the following formats when specifying the value for this parameter:  
  - SID  
  - DOMAIN\user-name  
  - user-name@DOMAIN  
  - user-name@FQDN  
  If you specify any of the three name formats for the value of -owner, keep in mind that the value is case insensitive.  
  The value for the -owner parameter is ignored for Storage-Level Access Guard. |
### Optional parameter

<table>
<thead>
<tr>
<th>Optional parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-group name_or_SID</td>
<td><strong>Primary Group of the Owner</strong></td>
</tr>
<tr>
<td></td>
<td>Specifies the owner group of the security descriptor. You can specify the</td>
</tr>
<tr>
<td></td>
<td>owner group using either a group name or SID. You can use any of the</td>
</tr>
<tr>
<td></td>
<td>following formats when specifying the value for this parameter:</td>
</tr>
<tr>
<td></td>
<td>• SID</td>
</tr>
<tr>
<td></td>
<td>• DOMAIN\group-name</td>
</tr>
<tr>
<td></td>
<td>• group-name@DOMAIN</td>
</tr>
<tr>
<td></td>
<td>• group-name@FQDN</td>
</tr>
<tr>
<td></td>
<td>If you specify any of the three name formats for the value of -group,</td>
</tr>
<tr>
<td></td>
<td>keep in mind that the value is case insensitive.</td>
</tr>
<tr>
<td></td>
<td>The value for the -group parameter is ignored for Storage-Level Access</td>
</tr>
<tr>
<td></td>
<td>Guard.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Before you can use this parameter, you must change to</td>
</tr>
<tr>
<td></td>
<td>advanced privilege level.</td>
</tr>
<tr>
<td>-control-flags-raw</td>
<td><strong>Raw control flags</strong></td>
</tr>
<tr>
<td>Hex_integer</td>
<td>Specifies the control flags in the security descriptor.</td>
</tr>
<tr>
<td></td>
<td>The value for the -control-flags-raw parameter is ignored for Storage-Level</td>
</tr>
<tr>
<td></td>
<td>Access Guard.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Before you can use this parameter, you must change to</td>
</tr>
<tr>
<td></td>
<td>advanced privilege level.</td>
</tr>
</tbody>
</table>

### Steps

1. If you want to use advanced parameters, set the privilege level to advanced:
   ```
   set -privilege advanced
   ```

2. Create a security descriptor:
   ```
   vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_name optional_parameters
   ```

   **Example**
   ```
   vserver security file-directory ntfs create -ntfs-sd sdl -vserver vs1 -owner domain\joe
   ```

3. Verify that security descriptor configuration is correct:
   ```
   vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name
   ```

   **Example**
   ```
   vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sdl
   ```

   **Vserver: vs1**
   Security Descriptor Name: sdl
   Owner of the Security Descriptor: DOMAIN\joe

4. If you are in advanced privilege level, return to the admin privilege level:
   ```
   set -privilege admin
   ```
Adding NTFS DACL access control entries to the NTFS security descriptor

Adding DACL (discretionary access control list) access control entries (ACEs) to the NTFS security descriptor is the second step in configuring and applying NTFS ACLs to a file or folder. Each entry identifies which object is allowed or denied access, and defines what the object can or cannot do to the files or folders defined in the ACE.

About this task

You can add one or more ACEs to the security descriptor's DACL.

If the security descriptor contains a DACL that has existing ACEs, the command adds the new ACE to the DACL. If the security descriptor does not contain a DACL, the command creates the DACL and adds the new ACE to it.

When adding an ACE to the DACL, you must provide information for the following four required parameters:

<table>
<thead>
<tr>
<th>Required parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-vserver vserver_name</td>
<td>SVM name</td>
</tr>
<tr>
<td>-ntfs-sd SD_name</td>
<td>Security descriptor</td>
</tr>
<tr>
<td>-access-type {deny</td>
<td>allow}</td>
</tr>
<tr>
<td>-account name_or_SID</td>
<td>Account</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

You can optionally customize DACL entries by specifying what rights you want to allow or deny for the account specified in the -account parameter. There are three mutually exclusive methods for specifying rights:

- Rights
- Advanced rights
- Raw rights (advanced-privilege)
### Optional rights parameters

<table>
<thead>
<tr>
<th>-rights</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no-access</td>
<td>Rights</td>
</tr>
<tr>
<td>full-control</td>
<td></td>
</tr>
<tr>
<td>modify</td>
<td></td>
</tr>
<tr>
<td>read-and-execute</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td></td>
</tr>
<tr>
<td>write</td>
<td></td>
</tr>
</tbody>
</table>

### Advanced rights

<table>
<thead>
<tr>
<th>-advanced-rights [advanced_access_right]</th>
<th>Advanced rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can specify one or more of the following advanced-right values by using a comma-delimited list:</td>
<td></td>
</tr>
<tr>
<td>• read-data</td>
<td></td>
</tr>
<tr>
<td>• write-data</td>
<td></td>
</tr>
<tr>
<td>• append-data</td>
<td></td>
</tr>
<tr>
<td>• read-ea</td>
<td></td>
</tr>
<tr>
<td>• write-ea</td>
<td></td>
</tr>
<tr>
<td>• execute-file</td>
<td></td>
</tr>
<tr>
<td>• delete-child</td>
<td></td>
</tr>
<tr>
<td>• read-attr</td>
<td></td>
</tr>
<tr>
<td>• write-attr</td>
<td></td>
</tr>
<tr>
<td>• delete</td>
<td></td>
</tr>
<tr>
<td>• read-perm</td>
<td></td>
</tr>
<tr>
<td>• write-perm</td>
<td></td>
</tr>
<tr>
<td>• write-owner</td>
<td></td>
</tr>
<tr>
<td>• full control</td>
<td></td>
</tr>
</tbody>
</table>

### Raw rights

<table>
<thead>
<tr>
<th>-raw-rights [Hex_integer]</th>
<th>Raw rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can specify raw rights as a Hex integer. Available in advanced mode only.</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** This is an advanced privilege level parameter. Before you can use this parameter, you must change to advanced privilege level by using the `set -privilege advanced` command.

**Note:** If you do not specify rights for the DACL entry, the default is to set the rights to **Full Control**.

You can optionally customize DACL entries by specifying how to apply inheritance.
Optional apply to parameter | Description
--- | ---
-apply-to {this-folder|sub-folder|files} | Apply DACL entry to
You can choose one or more of the parameter values by entering a comma-delimited list. If you do not specify this parameter, the default is to apply this DACL entry to this folder, subfolders, and files.
The following combinations of values for the -apply-to parameter are valid for Storage-Level Access Guard:
• this-folder, sub-folder, files
• this-folder, sub-folder
• files
Note: If you are configuring DACLs for security descriptors that you will associate with Storage-Level Access Guard tasks and you specify an invalid value for the -apply-to parameter for Storage-Level Access Guard, the security descriptor to which the DACL is associated is removed from any associated Storage-Level Access Guard task.

Steps
1. Add a DACL entry to a security descriptor:

   vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID optional_parameters

   **Example**

   vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny -account domain\joe -rights full-control -apply-to this-folder -vserver vs1

2. Verify that the DACL entry is correct:

   vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID

   **Example**

   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1 -access-type deny -account domain\joe

   Vserver: vs1
   Security Descriptor Name: sd1
   Allow or Deny: deny
   Account Name or SID: DOMAIN\joe
   Access Rights: full-control
   Advanced Access Rights: --
   Apply To: this-folder
   Access Rights: full-control

Creating a security policy

Creating a security policy for Storage Virtual Machines (SVMs) with FlexVol volumes is the third step in configuring and applying ACLs to a file or folder. A policy acts as a container for various
About this task

The tasks that you add to the security policy contain associations between NTFS security descriptor and file or folder paths; therefore, you should associate the policy with each SVM with FlexVol volumes (containing NTFS or mixed security-style volumes).

There are only two parameters for this command, and both are required.

<table>
<thead>
<tr>
<th>Required parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-vserver vserver_name</td>
<td>SVM name The name of the SVM that contains the files and folders with which you want to associate the policy.</td>
</tr>
<tr>
<td>-policy-name policy_name</td>
<td>policy_name The name of the security policy.</td>
</tr>
</tbody>
</table>

Steps

1. Create a security policy:

   `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   Example

   `vserver security file-directory policy create -policy-name policy1 -vserver vs1`

2. Verify the security policy:

   `vserver security file-directory policy show`

   Example

   `vserver security file-directory policy show`

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Policy Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>policy1</td>
</tr>
</tbody>
</table>

Adding a task to the security policy

Creating and adding a policy task to a security policy is the fourth step in configuring and applying ACLs to files or folders in Storage Virtual Machines (SVMs) with FlexVol volumes. When you create the policy task, you associate the task with a security policy. You can add one or more task entries to a security policy.

About this task

The security policy is a container for a task. A task refers to a single operation that can be done by a security policy to files or folders with NTFS or mixed security (or to a volume object if configuring Storage-Level Access Guard).

There are two types of tasks:

- File and directory tasks
Used to specify tasks that apply security descriptors to specified files and folders. ACLs applied through file and directory tasks can be managed with SMB clients or the Data ONTAP CLI.

- **Storage-Level Access Guard tasks**
  Used to specify tasks that apply Storage-Level Access Guard security descriptors to a specified volume. ACLs applied through Storage-Level Access Guard tasks can be managed only through the Data ONTAP CLI.

A task contains definitions for the security configuration of a file (or folder) or set of files (or folders). Every task in a policy is uniquely identified by the path. There can be only one task per path within a single policy. A policy cannot have duplicate task entries.

When adding a task to a policy, you should be aware of the following considerations:

- There can be a maximum of 10,000 tasks entries per policy.
- A policy can contain one or more tasks.
  Even though a policy can contain more than one task, you cannot configure a policy to contain both file-directory and Storage-Level Access Guard tasks. A policy must contain either all Storage-Level Access Guard tasks or all file-directory tasks.
- Storage-Level Access Guard is used to restrict permissions.
  It will never give extra access permissions.

When adding tasks to security policies, you must specify the following four required parameters:

<table>
<thead>
<tr>
<th>Required parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-vserver vserver_name</td>
<td><em>SVM name</em> Name of the SVM that contains the path to which you want to apply the security descriptor.</td>
</tr>
<tr>
<td>-policy-name policy_name</td>
<td><em>Policy name</em> Name of the security policy to which you want to add the task.</td>
</tr>
<tr>
<td>-path path</td>
<td><em>Path</em> Path on which to apply the security descriptor associated with this task.</td>
</tr>
<tr>
<td>-ntfs-sd SD_name</td>
<td><em>Security descriptor</em> The name of the security descriptor that you want to associate with the path in the task. Because it is required parameter, it is recommended that you create the security descriptor and add DACL ACEs (access control entries) and SACL ACEs (if desired) prior to creating the task, then associate the security descriptor with the file or folder path in the task, and finally add the task to the security policy. A security descriptor can contain multiple ACEs, both DACL ACEs and SACL ACEs.</td>
</tr>
</tbody>
</table>

You can customize the security descriptor configuration by using the following optional parameters:
<table>
<thead>
<tr>
<th>Optional parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| `-security-type`  | Security type  
Whether the security descriptor associated with this task is an NTFS or a NFSv4 security descriptor type. If you do not specify a value for this optional parameter, the default is `ntfs`.  
**Note:** The `nfsv4` security descriptor type is not supported in this release. If you specify this optional parameter, you must enter `ntfs` for the value of the `-security-type` parameter. |
| `-ntfs-mode`       | Propagation mode  
Specifies how to propagate security settings to child subfolders and files. This setting determines how child files and folders contained within a parent folder inherit access control and audit information from the parent folder. The three parameters correspond to three types of propagation modes:  
**Propagate**  
Propagates inheritable permissions to all subfolders and files. Existing permissions are not replaced.  
**Replace**  
Replaces existing permissions on all subfolders and files with inheritable permissions.  
**Ignore**  
Prevents permissions on this file or folder from being replaced.  
If this parameter is not specified, the default value is `propagate`.  
Because Storage-Level Access Guard security settings are automatically propagated to all files and folders within the volume, this setting is ignored if the task is a Storage-Level Access Guard task.  
**Note:** When volumes are mounted under a volume junction path and if Storage-Level Access Guard is present on that path, it will not be propagated for volumes mounted under it. |
| `-index-number`    | Index position  
Specifies the index number of a task. Tasks are applied in order. A task with a larger index number is applied after a task with a lower index number. If you do not specify this optional parameter, new tasks are applied to the end of the index list.  
The range of supported values is 1 through 9999. If there is a gap between the highest existing index number and the value entered for this parameter, the task with this number is considered to be the last task in the policy and is treated as having an index number of the previous highest index plus one.  
**Note:** If you specify an index number that is already assigned to an existing task, the task is added with that index number and the existing task index number is automatically arranged to the next number in the table. |
Optional parameter | Description
--- | ---
`-access-control [file-directory|slag]` | Access control type
Specifies the access control type of the task.
The default value is `file-directory`.
You must specify the access control type as `slag` if you adding a Storage-Level Access Guard task.
When the value is set to `slag`, the specified security descriptors with the task are applied for the volume specified in the `-path` parameter. Otherwise, the security descriptors are applied on files and directories as the specified path.

Steps

1. Add a task with an associated security descriptor to the security policy:

   ```bash
   vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_name optional_parameters
   ```

   `-access-control file-directory` is the default value for the `-access-control` parameter. Specifying the access control type when configuring file and directory access tasks is optional.

   **Example**

   ```bash
   vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
   ```

2. Verify the policy task configuration:

   ```bash
   vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path
   ```

   **Example**

   ```bash
   vserver security file-directory policy task show
   ```

<table>
<thead>
<tr>
<th>Index</th>
<th>File/Folder</th>
<th>Access Control</th>
<th>Security Type</th>
<th>NTFS Mode</th>
<th>NTFS Security Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>/home/dir1</td>
<td>file-directory</td>
<td>ntfs</td>
<td>propagate</td>
<td>sd2</td>
</tr>
</tbody>
</table>

**Applying security policies**

Applying a security policy to Storage Virtual Machines (SVMs) with FlexVol volumes is the last step to creating and applying NTFS ACLs to files or folders.

**About this task**

You can apply security settings defined in the security policy to NTFS files and folders residing within FlexVol volumes (NTFS or mixed security style).
### Required parameters

<table>
<thead>
<tr>
<th>Required parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-vserver vserver_name</code></td>
<td>The name of the SVM that contains the files and folders to which you want to apply the policy with its associated task.</td>
</tr>
<tr>
<td><code>-policy-name policy_name</code></td>
<td>The name of the security policy to apply.</td>
</tr>
</tbody>
</table>

### Step

1. Apply a security policy:

   ```bash
   vserver security file-directory policy apply -vserver vserver_name -policy-name policy_name
   ```

   **Example**

   ```bash
   vserver security file-directory policy apply -vserver vs1 -policy-name policy1
   ```

   The policy apply job is scheduled.

### Monitoring the security policy job

When applying the security policy to Storage Virtual Machines (SVMs) with FlexVol volumes, you can monitor the progress of the task by monitoring the security policy job. This is helpful if you want to ascertain that the application of the security policy succeeded. This is also helpful if you have a long-running job where you are applying bulk security to a large number of files and folders.

### About this task

To display detailed information about a security policy job, use the `-instance` parameter.

### Step

1. Monitor the security policy job:

   ```bash
   vserver security file-directory job show -vserver vserver_name
   ```

   **Example**

   ```bash
   vserver security file-directory job show -vserver vs1
   ```

<table>
<thead>
<tr>
<th>Job ID</th>
<th>Name</th>
<th>Vserver</th>
<th>Node</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>53322</td>
<td>Fsecurity Apply</td>
<td>vs1</td>
<td>node1</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>Description: File Directory Security Apply Job</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Verifying the applied file security

You can verify the file security settings to confirm that the files or folders on the Storage Virtual Machine (SVM) with FlexVol volumes to which you applied the security policy have the desired settings.

### About this task

You must supply the name of the SVM that contains the data and the path to the file and folders on which you want to verify security settings. You can use the optional `-expand-mask` parameter to display detailed information about the security settings.
Step

1. Display file and folder security settings:

   vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]

Example

   vserver security file-directory show -vserver vs1 -path /data/engineering -expand-mask true

| Vserver: vs1                                      |
| File Path: /data/engineering                      |
| File Inode Number: 5544                           |
| Security Style: ntfs                               |
| Effective Style: ntfs                             |
| DOS Attributes: 10                                |
| DOS Attributes in Text: D---                      |
| Expanded Dos Attributes: 0x10                     |
| ...0 .... .... .... = Offline                      |
| ....0 .... .... .... = Sparse                      |
| ....0 .... .... .... = Normal                      |
| ....0 .... .... .... = Archive                     |
| ....0 .... .... .... = Directory                   |
| ....0 .... .... .... = System                      |
| ....0 .... .... .... = Hidden                      |
| ....0 .... .... .... = Read Only                   |
| Unix User Id: 0                                   |
| Unix Group Id: 0                                  |
| Unix Mode Bits: 777                               |
| Unix Mode Bits in Text: rwrxrwx                    |
| ACLs: NTFS Security Descriptor                    |
| Control:0x8004                                    |
| 1... .... .... .... = Self Relative                |
| ....0 .... .... .... = RM Control Valid            |
| ....0 .... .... .... = DACL Protected              |
| ....0 .... .... .... = DACL Inherited              |
| ....0 .... .... .... = SACL Inherited              |
| ....0 .... .... .... = DACL Inherit Required       |
| ....0 .... .... .... = SACL Inherit Required       |
| ....0 .... .... .... = DACL Defaulted              |
| ....0 .... .... .... = SACL Defaulted              |
| Owner:BUILTIN\Administrators                      |
| Group:BUILTIN\Administrators                      |
| DACL - ACEs                                       |
| ALLOW-Everyone-0x1f01ff                           |
| 0... .... .... .... .... = Generic Read             |
| ....0 .... .... .... .... = Generic Write           |
| ....0 .... .... .... .... = Generic Execute         |
| ....0 .... .... .... .... = System Security         |
| ....0 .... .... .... .... = Synchronize             |
| ....0 .... .... .... .... = Read Control            |
| ....0 .... .... .... .... = Delete                  |
| ....0 .... .... .... .... = Write Attributes        |
| ....0 .... .... .... .... = Read Attributes         |
| ....0 .... .... .... .... = Write EA                |
| ....0 .... .... .... .... = Read EA                 |
| ....0 .... .... .... .... = Delete                  |
| ....0 .... .... .... .... = Write Attributes        |
| ....0 .... .... .... .... = Read Attributes         |

Managing file access using SMB | 267
Configuring and applying audit policies on NTFS files and folders using the CLI

There are several steps you must perform to apply audit policies to NTFS files and folders when using the Data ONTAP CLI. First, you create an NTFS security descriptor and add SACLs to the security descriptor. Next you create a security policy and add policy tasks. You then apply the security policy to a Storage Virtual Machine (SVM) with FlexVol volumes.

About this task

After applying the security policy, you can monitor the security policy job and then verify the settings on the applied audit policy.

Steps

1. Creating an NTFS security descriptor on page 269
   Creating an NTFS security descriptor is the first step in configuring and applying NTFS access control lists (ACLs) to files and folders residing within Storage Virtual Machines (SVMs) with FlexVol volumes. You will associate the security descriptor to the file or folder path in a policy task.

2. Adding NTFS SACL access control entries to the NTFS security descriptor on page 271
   Adding SACL (system access control list) access control entries (ACEs) to the NTFS security descriptor is the second step in creating NTFS audit policies for files or folders in Storage Virtual Machine (SVM) with FlexVol volumes. Each entry identifies the user or group that you want to audit. The SACL entry defines whether you want to audit successful or failed access attempts.

3. Creating a security policy on page 274
   Creating a security policy for Storage Virtual Machines (SVMs) with FlexVol volumes is the third step in configuring and applying ACLs to a file or folder. A policy acts as a container for various tasks where each task is a single entry that can be applied to files or folders. You later add tasks to the security policy.

4. Adding a task to the security policy on page 275
   Creating and adding a policy task to a security policy is the fourth step in configuring and applying ACLs to files or folders in Storage Virtual Machines (SVMs) with FlexVol volumes. When you create the policy task, you associate the task with a security policy. You can add one or more task entries to a security policy.

5. Applying security policies on page 278
   Applying a security policy to Storage Virtual Machines (SVMs) with FlexVol volumes is the last step to creating and applying NTFS ACLs to files or folders.

6. Monitoring the security policy job on page 279
   When applying the security policy to Storage Virtual Machines (SVMs) with FlexVol volumes, you can monitor the progress of the task by monitoring the security policy job. This is helpful if you want to ascertain that the application of the security policy succeeded. This is also helpful if you have a long-running job where you are applying bulk security to a large number of files and folders.

7. Verifying the applied audit policy on page 279
   You can verify the audit policy to confirm that the files or folders on the Storage Virtual Machine (SVM) with FlexVol volumes to which you applied the security policy have the desired audit security settings.
Creating an NTFS security descriptor

Creating an NTFS security descriptor is the first step in configuring and applying NTFS access control lists (ACLs) to files and folders residing within Storage Virtual Machines (SVMs) with FlexVol volumes. You will associate the security descriptor to the file or folder path in a policy task.

About this task

You can create NTFS security descriptors for files and folders residing within NTFS security-style volumes, or for files and folders residing on mixed security-style volumes.

By default, when a security descriptor is created, four discretionary access control list (DACL) access control entries (ACEs) are added to that security descriptor. The four default ACEs are as follows:

<table>
<thead>
<tr>
<th>Object</th>
<th>Access type</th>
<th>Access rights</th>
<th>Where to apply the permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>BUILTIN\Administrators</td>
<td>Allow</td>
<td>Full Control</td>
<td>this-folder, sub-folders, files</td>
</tr>
<tr>
<td>BUILTIN\Users</td>
<td>Allow</td>
<td>Full Control</td>
<td>this-folder, sub-folders, files</td>
</tr>
<tr>
<td>CREATOR OWNER</td>
<td>Allow</td>
<td>Full Control</td>
<td>this-folder, sub-folders, files</td>
</tr>
<tr>
<td>NT AUTHORITY \SYSTEM</td>
<td>Allow</td>
<td>Full Control</td>
<td>this-folder, sub-folders, files</td>
</tr>
</tbody>
</table>

When creating the security descriptor, you must specify the following two parameters:

<table>
<thead>
<tr>
<th>Required parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-vserver vserver_name</td>
<td>SVM name</td>
</tr>
<tr>
<td></td>
<td>The name of the SVM that contains the files and folders to which you want to apply the security descriptor.</td>
</tr>
<tr>
<td>-ntfs-sd SD_name</td>
<td>Security descriptor</td>
</tr>
<tr>
<td></td>
<td>The name to assign to the security descriptor.</td>
</tr>
</tbody>
</table>

You can customize the security descriptor configuration by using the following optional parameters:
### Optional parameter | Description
--- | ---
-`owner name_or_SID` | **Owner of the security descriptor**
The owner of the security descriptor can modify the permissions on the files (or folders) to which the security descriptor is applied and can give other users the right to take ownership of the objects to which the security descriptor is applied. You can use any of the following formats when specifying the value for this parameter:

- SID
- `DOMAIN\user-name`
- `user-name@DOMAIN`
- `user-name@FQDN`

If you specify any of the three name formats for the value of `-owner`, keep in mind that the value is case insensitive.
The value for the `-owner` parameter is ignored for Storage-Level Access Guard.

-`group name_or_SID` | **Primary Group of the Owner**
Specifies the owner group of the security descriptor. You can specify the owner group using either a group name or SID. You can use any of the following formats when specifying the value for this parameter:

- SID
- `DOMAIN\group-name`
- `group-name@DOMAIN`
- `group-name@FQDN`

If you specify any of the three name formats for the value of `-group`, keep in mind that the value is case insensitive.
The value for the `-group` parameter is ignored for Storage-Level Access Guard.

#### Note: Before you can use this parameter, you must change to advanced privilege level.

-`control-flags-raw Hex_integer` | **Raw control flags**
Specifies the control flags in the security descriptor.
The value for the `-control-flags-raw` parameter is ignored for Storage-Level Access Guard.

#### Note: Before you can use this parameter, you must change to advanced privilege level.

### Steps
1. If you want to use advanced parameters, set the privilege level to advanced:
   ```
   set -privilege advanced
   ```
2. Create a security descriptor:
   ```
   vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_name optional_parameters
   ```
Example

```
vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner domain\joe
```

3. Verify that security descriptor configuration is correct:

```
vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name
```

Example

```
vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
```

<table>
<thead>
<tr>
<th>Vserver: vs1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Descriptor Name: sd1</td>
</tr>
<tr>
<td>Owner of the Security Descriptor: DOMAIN\joe</td>
</tr>
</tbody>
</table>

4. If you are in advanced privilege level, return to the admin privilege level:

```
set -privilege admin
```

**Adding NTFS SACL access control entries to the NTFS security descriptor**

Adding SACL (system access control list) access control entries (ACEs) to the NTFS security descriptor is the second step in creating NTFS audit policies for files or folders in Storage Virtual Machine (SVM) with FlexVol volumes. Each entry identifies the user or group that you want to audit. The SACL entry defines whether you want to audit successful or failed access attempts.

**About this task**

You can add one or more ACEs to the security descriptor's SACL.

If the security descriptor contains a SACL that has existing ACEs, the command adds the new ACE to the SACL. If the security descriptor does not contain a SACL, the command creates the SACL and adds the new ACE to it.

When adding an ACE to the SACL, you must provide information for the following four required parameters:

<table>
<thead>
<tr>
<th>Required parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-vserver vserver_name</code></td>
<td><em>SVM name</em> The name of the SVM that contains the files and folders to which the security descriptor is applied.</td>
</tr>
<tr>
<td><code>-ntfs-sd SD_name</code></td>
<td><em>Security descriptor</em> The name of the security descriptor to which you want to add SACL entries.</td>
</tr>
<tr>
<td>`-access-type [failure</td>
<td>success]`</td>
</tr>
</tbody>
</table>
### Required parameters

<table>
<thead>
<tr>
<th>Required parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-account</code> name_or_SID</td>
<td><strong>Account</strong>&lt;br&gt;The account on which to apply the system ACE. You can specify the account by using a user name or a SID. You can use any of the following formats when specifying the value for this parameter:&lt;br&gt;- SID&lt;br&gt;- DOMAIN\user-name&lt;br&gt;- user-name@DOMAIN&lt;br&gt;- user-name@FQDN&lt;br&gt;If you specify any of the three name formats for the value of <code>-account</code>, keep in mind that the value is not case-sensitive.</td>
</tr>
</tbody>
</table>

You can configure SACL entries by specifying what rights you want to audit for success or failure events for the account specified in the `-account` parameter. There are three mutually exclusive methods for specifying rights:

- Rights
- Advanced rights
- Raw rights (advanced-privilege)

To audit events, configure one of the three rights parameters:

<table>
<thead>
<tr>
<th>Optional rights parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-rights</code> no-access</td>
<td>full-control</td>
</tr>
<tr>
<td>Optional rights parameters</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| `-advanced-rights` `advanced_access_right` |  **Advanced rights**  
You can specify one or more of the following advanced-right values by using a comma-delimited list:  
- read-data  
- write-data  
- append-data  
- read-ea  
- write-ea  
- execute-file  
- delete-child  
- read-attr  
- write-attr  
- delete  
- read-perm  
- write-perm  
- write-owner  
- full control |
| `-raw-rights` `Hex_integer` |  **Raw rights**  
You can specify raw rights as a Hex integer. Available in advanced mode only.  
**Note:** This is an advanced-privilege-level parameter. Before you can use this parameter, you must change to advanced privilege level by using the following command:  
`set -privilege advanced` |

**Note:** If you do not specify rights for the SACL entry, the default setting is **Full Control**.

You can optionally customize SACL entries by specifying how to apply inheritance with the `apply to` parameter. If you do not specify this parameter, the default is to apply this SACL entry to this folder, subfolders, and files.
Optional apply to parameter | Description
-----------------------------|----------------------------------------
-apply-to {this-folder|sub-folder|files} | Apply SACL entry to
You can choose one or more of the parameter values by entering a comma-delimited list.
The following combinations of values for the -apply-to parameter are valid for Storage-Level Access Guard:
• this-folder, sub-folder, files
• this-folder, sub-folder
• files

Note: If you are configuring SACLs for security descriptors that you will associate with Storage-Level Access Guard tasks and you specify an invalid value for the -apply-to parameter for Storage-Level Access Guard, the security descriptor to which the SACL is associated is removed from any associated Storage-Level Access Guard task.

Steps
1. Add a SACL entry to a security descriptor:

   vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID optional_parameters

   Example

   vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type failure -account domain\joe -rights full-control -apply-to this-folder -vserver vs1

2. Verify that the SACL entry is correct:

   vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID

   Example

   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1 -access-type deny -account domain\joe

   | Vserver: vs1 |
   | Security Descriptor Name: sd1 |
   | Access type for Specified Access Rights: failure |
   | Account Name or SID: DOMAIN\joe |
   | Advanced Access Rights: - |
   | Apply To: this-folder |
   | Access Rights: full-control |

Creating a security policy

Creating a security policy for Storage Virtual Machines (SVMs) with FlexVol volumes is the third step in configuring and applying ACLs to a file or folder. A policy acts as a container for various
tasks where each task is a single entry that can be applied to files or folders. You later add tasks to the security policy.

About this task

The tasks that you add to the security policy contain associations between NTFS security descriptor and file or folder paths; therefore, you should associate the policy with each SVM with FlexVol volumes (containing NTFS or mixed security-style volumes).

There are only two parameters for this command, and both are required.

<table>
<thead>
<tr>
<th>Required parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-vserver vserver_name</td>
<td>SVM name</td>
</tr>
<tr>
<td>vserver_name</td>
<td>The name of the SVM that contains the files and folders with which you want to associate the policy.</td>
</tr>
<tr>
<td>-policy-name policy_name</td>
<td>policy_name</td>
</tr>
<tr>
<td>policy_name</td>
<td>The name of the security policy.</td>
</tr>
</tbody>
</table>

Steps

1. Create a security policy:

   vserver security file-directory policy create -vserver vserver_name -policy-name policy_name

   Example

   vserver security file-directory policy create -policy-name policy1 -vserver vs1

2. Verify the security policy:

   vserver security file-directory policy show

   Example

   vserver security file-directory policy show

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Policy Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>policy1</td>
</tr>
</tbody>
</table>

Adding a task to the security policy

Creating and adding a policy task to a security policy is the fourth step in configuring and applying ACLs to files or folders in Storage Virtual Machines (SVMs) with FlexVol volumes. When you create the policy task, you associate the task with a security policy. You can add one or more task entries to a security policy.

About this task

The security policy is a container for a task. A task refers to a single operation that can be done by a security policy to files or folders with NTFS or mixed security (or to a volume object if configuring Storage-Level Access Guard).

There are two types of tasks:

- File and directory tasks
Used to specify tasks that apply security descriptors to specified files and folders. ACLs applied through file and directory tasks can be managed with SMB clients or the Data ONTAP CLI.

- **Storage-Level Access Guard tasks**
  Used to specify tasks that apply Storage-Level Access Guard security descriptors to a specified volume. ACLs applied through Storage-Level Access Guard tasks can be managed only through the Data ONTAP CLI.

A task contains definitions for the security configuration of a file (or folder) or set of files (or folders). Every task in a policy is uniquely identified by the path. There can be only one task per path within a single policy. A policy cannot have duplicate task entries.

When adding a task to a policy, you should be aware of the following considerations:

- There can be a maximum of 10,000 tasks entries per policy.
- A policy can contain one or more tasks.
  Even though a policy can contain more than one task, you cannot configure a policy to contain both file-directory and Storage-Level Access Guard tasks. A policy must contain either all Storage-Level Access Guard tasks or all file-directory tasks.
- **Storage-Level Access Guard is used to restrict permissions.**
  It will never give extra access permissions.

When adding tasks to security policies, you must specify the following four required parameters:

<table>
<thead>
<tr>
<th>Required parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-vserver vserver_name</td>
<td><strong>SVM name</strong> Name of the SVM that contains the path to which you want to apply the security descriptor.</td>
</tr>
<tr>
<td>-policy-name policy_name</td>
<td><strong>Policy name</strong> Name of the security policy to which you want to add the task.</td>
</tr>
<tr>
<td>-path path</td>
<td><strong>Path</strong> Path on which to apply the security descriptor associated with this task.</td>
</tr>
<tr>
<td>-ntfs-sd SD_name</td>
<td><strong>Security descriptor</strong> The name of the security descriptor that you want to associate with the path in the task.</td>
</tr>
</tbody>
</table>
  Because it is required parameter, it is recommended that you create the security descriptor and add DACL ACEs (access control entries) and SACL ACEs (if desired) prior to creating the task, then associate the security descriptor with the file or folder path in the task, and finally add the task to the security policy. A security descriptor can contain multiple ACEs, both DACL ACEs and SACL ACEs. |

You can customize the security descriptor configuration by using the following optional parameters:
<table>
<thead>
<tr>
<th>Optional parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| `-security-type`  | *Security type*  
Whether the security descriptor associated with this task is an NTFS or a NFSv4 security descriptor type. If you do not specify a value for this optional parameter, the default is `ntfs`.  
**Note:** The `nfsv4` security descriptor type is not supported in this release.  
If you specify this optional parameter, you must enter `ntfs` for the value of the `-security-type` parameter. |
| `-ntfs-mode`      | *Propagation mode*  
Specifies how to propagate security settings to child subfolders and files. This setting determines how child files and folders contained within a parent folder inherit access control and audit information from the parent folder. The three parameters correspond to three types of propagation modes:  
**Propagate**  
Propagates inheritable permissions to all subfolders and files. Existing permissions are not replaced.  
**Replace**  
Replaces existing permissions on all subfolders and files with inheritable permissions.  
**Ignore**  
Prevents permissions on this file or folder from being replaced.  
If this parameter is not specified, the default value is `propagate`.  
Because Storage-Level Access Guard security settings are automatically propagated to all files and folders within the volume, this setting is ignored if the task is a Storage-Level Access Guard task.  
**Note:** When volumes are mounted under a volume junction path and if Storage-Level Access Guard is present on that path, it will not be propagated for volumes mounted under it. |
| `-index-number`   | *Index position*  
Specifies the index number of a task. Tasks are applied in order. A task with a larger index number is applied after a task with a lower index number. If you do not specify this optional parameter, new tasks are applied to the end of the index list.  
The range of supported values is 1 through 9999. If there is a gap between the highest existing index number and the value entered for this parameter, the task with this number is considered to be the last task in the policy and is treated as having an index number of the previous highest index plus one.  
**Note:** If you specify an index number that is already assigned to an existing task, the task is added with that index number and the existing task index number is automatically arranged to the next number in the table. |
**Optional parameter** | **Description**
---|---
`--access-control {file-directory|slag}` | *Access control type*
Specifies the access control type of the task.
The default value is `file-directory`.
You must specify the access control type as `slag` if you adding a Storage-Level Access Guard task.
When the value is set to `slag`, the specified security descriptors with the task are applied for the volume specified in the `--path` parameter. Otherwise, the security descriptors are applied on files and directories as the specified path.

**Steps**

1. Add a task with an associated security descriptor to the security policy:

   ```bash
   vserver security file-directory policy task add --vserver vserver_name --policy-name policy_name --path path --ntfs-sd SD_name optional_parameters
   ```

   *file-directory* is the default value for the `--access-control` parameter. Specifying the access control type when configuring file and directory access tasks is optional.

   **Example**

   ```bash
   vserver security file-directory policy task add --vserver vs1 --policy-name policy1 --path /home/dir1 --security-type ntfs --ntfs-mode propagate --ntfs-sd sd2 --index-num 1 --access-control file-directory
   ```

2. Verify the policy task configuration:

   ```bash
   vserver security file-directory policy task show --vserver vserver_name --policy-name policy_name --path path
   ```

   **Example**

   ```bash
   vserver security file-directory policy task show
   ```

<table>
<thead>
<tr>
<th>Vserver: vs1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy: policy1</td>
</tr>
<tr>
<td>Index</td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td>1</td>
</tr>
</tbody>
</table>

**Applying security policies**

Applying a security policy to Storage Virtual Machines (SVMs) with FlexVol volumes is the last step to creating and applying NTFS ACLs to files or folders.

**About this task**

You can apply security settings defined in the security policy to NTFS files and folders residing within FlexVol volumes (NTFS or mixed security style).
### Required parameters

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>-vserver</strong></td>
</tr>
<tr>
<td><strong>-policy-name</strong></td>
</tr>
</tbody>
</table>

### Step

1. Apply a security policy:

   ```
   vserver security file-directory policy apply -vserver vserver_name -policy-name policy_name
   ```

   **Example**

   ```
   vserver security file-directory apply -vserver vs1 -policy-name policy1
   ```

   The policy apply job is scheduled.

### Monitoring the security policy job

When applying the security policy to Storage Virtual Machines (SVMs) with FlexVol volumes, you can monitor the progress of the task by monitoring the security policy job. This is helpful if you want to ascertain that the application of the security policy succeeded. This is also helpful if you have a long-running job where you are applying bulk security to a large number of files and folders.

#### About this task

To display detailed information about a security policy job, use the `-instance` parameter.

### Step

1. Monitor the security policy job:

   ```
   vserver security file-directory job show -vserver vserver_name
   ```

   **Example**

   ```
   vserver security file-directory job show -vserver vs1
   ```

<table>
<thead>
<tr>
<th>Job ID</th>
<th>Name</th>
<th>Vserver</th>
<th>Node</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>53322</td>
<td>Fsecurity Apply</td>
<td>vs1</td>
<td>node1</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>Description: File Directory Security Apply Job</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Verifying the applied audit policy

You can verify the audit policy to confirm that the files or folders on the Storage Virtual Machine (SVM) with FlexVol volumes to which you applied the security policy have the desired audit security settings.

#### About this task

You use the `vserver security file-directory show` command to display audit policy information. You must supply the name of the SVM that contains the data and the path to the data whose file or folder audit policy information you want to display.
Step

1. Display audit policy settings:

   `vserver security file-directory show -vserver vserver_name -path path`

Example

The following command displays the audit policy information applied to the path “/corp” in SVM vs1. The path has both a SUCCESS and a SUCCESS/FAIL SACL entry applied to it:

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp

Vserver: vs1
File Path: /corp
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
  Unix User Id: 0
  Unix Group Id: 0
  Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
  Control:0x8014
  Owner:DOMAIN\Administrator
  Group:BUILTIN\Administrators
  SACL - ACEs
    ALL-DOMAIN\Administrator-0x100081-OI|CI|
    SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
    DACL - ACEs
    ALLOW-BUILTIN\Administrators-0x1f01ff-OI|
    ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
    ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
    ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Considerations when managing security policy jobs

If a security policy job exists, under certain circumstances, you cannot modify that security policy or the tasks assigned to that policy. You should understand under what conditions you can or cannot modify security policies so that any attempts that you make to modify the policy are successful. Modifications to the policy include adding, removing, or modifying tasks assigned to the policy and deleting or modifying the policy.

You cannot modify a security policy or a task assigned to that policy if a job exists for that policy and that job is in the following states:

- The job is running or in progress.
- The job is paused.
- The job is resumed and is in the running state.
- If the job is waiting to failover to another node.

Under the following circumstances, if a job exists for a security policy, you can successfully modify that security policy or a task assigned to that policy:

- The policy job is stopped.
- The policy job has successfully finished.
### Commands for managing NTFS security descriptors

There are specific Data ONTAP commands for managing security descriptors. You can create, modify, delete, and display information about security descriptors.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create NTFS security descriptors</td>
<td><code>vserver security file-directory ntfs create</code></td>
</tr>
<tr>
<td>Modify existing NTFS security</td>
<td><code>vserver security file-directory ntfs modify</code></td>
</tr>
<tr>
<td>descriptors</td>
<td></td>
</tr>
<tr>
<td>Display information about existing</td>
<td><code>vserver security file-directory ntfs show</code></td>
</tr>
<tr>
<td>NTFS security descriptors</td>
<td></td>
</tr>
<tr>
<td>Delete NTFS security descriptors</td>
<td><code>vserver security file-directory ntfs delete</code></td>
</tr>
</tbody>
</table>

See the man pages for the `vserver security file-directory ntfs` commands for more information.

### Commands for managing NTFS DACL access control entries

There are specific Data ONTAP commands for managing DACL access control entries (ACEs). You can add ACEs to NTFS DACLs at any time. You can also manage existing NTFS DACLs by modifying, deleting, and displaying information about ACEs in DACLs.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create ACEs and add them to NTFS</td>
<td><code>vserver security file-directory ntfs dacl add</code></td>
</tr>
<tr>
<td>DACLs</td>
<td></td>
</tr>
<tr>
<td>Modify existing ACEs in NTFS DACLs</td>
<td><code>vserver security file-directory ntfs dacl modify</code></td>
</tr>
<tr>
<td>Display information about existing</td>
<td><code>vserver security file-directory ntfs dacl show</code></td>
</tr>
<tr>
<td>ACEs in NTFS DACLs</td>
<td></td>
</tr>
<tr>
<td>Remove existing ACEs from NTFS</td>
<td><code>vserver security file-directory ntfs dacl remove</code></td>
</tr>
<tr>
<td>DACLs</td>
<td></td>
</tr>
</tbody>
</table>

See the man pages for the `vserver security file-directory ntfs dacl` commands for more information.

### Commands for managing NTFS SACL access control entries

There are specific Data ONTAP commands for managing SACL access control entries (ACEs). You can add ACEs to NTFS SACLs at any time. You can also manage existing NTFS SACLs by modifying, deleting, and displaying information about ACEs in SACLs.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create ACEs and add them to NTFS</td>
<td><code>vserver security file-directory ntfs sacl add</code></td>
</tr>
<tr>
<td>SACLs</td>
<td></td>
</tr>
<tr>
<td>Modify existing ACEs in NTFS SACLs</td>
<td><code>vserver security file-directory ntfs sacl modify</code></td>
</tr>
<tr>
<td>Display information about existing</td>
<td><code>vserver security file-directory ntfs sacl show</code></td>
</tr>
<tr>
<td>ACEs in NTFS SACLs</td>
<td></td>
</tr>
</tbody>
</table>
If you want to... | Use this command...
---|---
Remove existing ACEs from NTFS SACLs | `vserver security file-directory ntfs sacl remove`

See the man pages for the `vserver security file-directory ntfs sacl remove` commands for more information.

### Commands for managing security policies

There are specific Data ONTAP commands for managing security policies. You can display information about policies and you can delete policies. You cannot modify a security policy.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create security policies</td>
<td><code>vserver security file-directory policy create</code></td>
</tr>
<tr>
<td>Display information about security policies</td>
<td><code>vserver security file-directory policy show</code></td>
</tr>
<tr>
<td>Delete security policies</td>
<td><code>vserver security file-directory policy delete</code></td>
</tr>
</tbody>
</table>

See the man pages for the `vserver security file-directory policy` commands for more information.

### Commands for managing security policy tasks

There are Data ONTAP commands for adding, modifying, removing, and displaying information about security policy tasks.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add security policy tasks</td>
<td><code>vserver security file-directory policy task add</code></td>
</tr>
<tr>
<td>Modify security policy tasks</td>
<td><code>vserver security file-directory policy task modify</code></td>
</tr>
<tr>
<td>Display information about security policy tasks</td>
<td><code>vserver security file-directory policy task show</code></td>
</tr>
<tr>
<td>Remove security policy tasks</td>
<td><code>vserver security file-directory policy task remove</code></td>
</tr>
</tbody>
</table>

See the man pages for the `vserver security file-directory policy task` commands for more information.

### Commands for managing security policy jobs

There are Data ONTAP commands for pausing, resuming, stopping, and displaying information about security policy jobs.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pause security policy jobs</td>
<td><code>vserver security file-directory job pause -vserver vserver_name -id integer</code></td>
</tr>
<tr>
<td>Resume security policy jobs</td>
<td><code>vserver security file-directory job resume -vserver vserver_name -id integer</code></td>
</tr>
</tbody>
</table>
If you want to... | Use this command...
--- | ---
Display information about security policy jobs | `vserver security file-directory job show -vserver vserver_name`
Stop security policy jobs | `vserver security file-directory job stop -vserver vserver_name -id integer`

You can determine the job ID of a job using this command.

See the man pages for the `vserver security file-directory job` commands for more information.

**Using security tracing to verify or troubleshoot file and directory access**

You can add permission tracing filters to instruct Data ONTAP to log information about why the CIFS server on a Storage Virtual Machine (SVM) with FlexVol volumes allows or denies a client or user's request to perform an operation. This can be useful when you want to verify that your file access security scheme is appropriate or when you want to troubleshoot file access issues.

**How security traces work**

Security traces allow you to configure a filter that detects client operations over SMB on the Storage Virtual Machine (SVM) with FlexVol volumes, and trace all access checks matching that filter. You can then view the trace results, which provides a convenient summary of the reason that access was allowed or denied.

When you want to verify the security settings for SMB access on files and folders on your SVM or if you are faced with an access problem, you can quickly add a filter to turn on permission tracing.

The following list outlines important facts about how security traces works:

- Data ONTAP applies security traces at the SVM level.
- Each incoming request is screened to see if it matches filtering criteria of any enabled security traces.
- Traces are performed for both file and folder access requests.
- Traces can filter based on the following criteria:
  - Client IP
  - SMB path
  - Windows name
  - UNIX name
- Requests are screened for *Allowed* and *Denied* access response results.
- Each request matching filtering criteria of enabled traces is recorded in the trace results log.
- The storage administrator can configure a timeout on a filter to automatically disable it.
- If a request matches multiple filters, the results from the filter with the highest index number is recorded.
- The storage administrator can print results from the trace results log to determine why an access request was allowed or denied.
Related concepts

- How to interpret security trace results on page 292
- How security styles affect data access on page 20

Related tasks

- Performing security traces on page 285

Types of access checks security traces monitor

Access checks for a file or folder are done based on multiple criteria. Security traces monitor operations on all these criteria.

The types of access checks that security traces monitor include the following:

- Volume and qtree security style
- Effective security of the file system containing the files and folders on which operations are requested
- User mapping
- Share-level permissions
- File-level permissions
- Storage-Level Access Guard security

Considerations when creating security traces

You should keep several considerations in mind when you create security traces on Storage Virtual Machines (SVMs) with FlexVol volumes. For example, you need to know on which protocols you can create a trace, which security-styles are supported, and what the maximum number of active traces is.

- You can only create security traces on SVMs with FlexVol volumes.
- Each security trace filter entry is SVM specific.
  You must specify the SVM on which you want to run the trace.
- You can add permission tracing filters for SMB requests only.
- You must set up the CIFS server on the SVM on which you want to create trace filters.
- You can create security traces for files and folders residing on NTFS, UNIX, and mixed security-style volumes and qtrees.
- You can add a maximum of 10 permission tracing filters per SVM.
- You must specify a filter index number when creating or modifying a filter.
  Filters are considered in order of the index number. The criteria in a filter with a higher index number is considered before the criteria with a lower index number. If the request being traced matches criteria in multiple enabled filters, only the filter with the highest index number is triggered.
- After you have created and enabled a security trace filter, you must perform some file or folder requests on a client system to generate activity that the trace filter can capture and log in the trace results log.
- You should add permission tracing filters for file access verification or troubleshooting purposes only.
  Adding permission tracing filters has a minor effect on controller performance.
When you are done with verification or troubleshooting activity, you should disable or remove all permission tracing filters. Furthermore, the filtering criteria you select should be as specific as possible so that Data ONTAP does not send a large number of trace results to the log.

**Performing security traces**

Performing a security trace involves creating a security trace filter, verifying the filter criteria, generating access requests on an SMB client that match filter criteria, and viewing the results.

**About this task**

After you are finished using a security filter to capture trace information, you can modify the filter and reuse it, or disable it if you no longer need it. After viewing and analyzing the filter trace results, you can then delete them if they are no longer needed.

**Steps**

1. **Creating security trace filters** on page 286
   You can create security trace filters that detect SMB client operations on Storage Virtual Machines (SVMs) with FlexVol volumes and trace all access checks matching the filter. You can use the results from security traces to validate your configuration or to troubleshoot access issues.

2. **Displaying information about security trace filters** on page 287
   You can display information about security trace filters configured on your Storage Virtual Machine (SVM). This enables you to see which types of access events each filter traces.

3. **Displaying security trace results** on page 288
   You can display the security trace results generated for file operations that match security trace filters. You can use the results to validate your file access security configuration or to troubleshoot SMB file access issues.

4. **Modifying security trace filters** on page 289
   If you want to change the optional filter parameters used to determine which access events are traced, you can modify existing security trace filters.

5. **Deleting security trace filters** on page 290
   When you no longer need a security trace filter entry, you can delete it. Because you can have a maximum of 10 security trace filters per Storage Virtual Machine (SVM), deleting unneeded filters enables you to create new filters if you have reached the maximum.

6. **Deleting security trace records** on page 291
   After you finish using a filter trace record to verify file access security or to troubleshoot SMB client access issues, you can delete the security trace record from the security trace log.

7. **Deleting all security trace records** on page 292
   If you do not want to keep any of the existing security trace records, you can delete all of the records on a node with a single command.

**Related concepts**

- *How security traces work* on page 283
- *Types of access checks security traces monitor* on page 284
- *Considerations when creating security traces* on page 284
- *How to interpret security trace results* on page 292
- *Displaying information about file security and audit policies* on page 240
Creating security trace filters

You can create security trace filters that detect SMB client operations on Storage Virtual Machines (SVMs) with FlexVol volumes and trace all access checks matching the filter. You can use the results from security traces to validate your configuration or to troubleshoot access issues.

About this task

There are two required parameters for this command:

<table>
<thead>
<tr>
<th>Required parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-vserver vserver_name</td>
<td>SVM name</td>
</tr>
<tr>
<td>-index index_number</td>
<td>Filter index number</td>
</tr>
</tbody>
</table>

The name of the SVM that contains the files or folders on which you want to apply the security trace filter.

The index number you want to apply to the filter. You are limited to a maximum of 10 trace filters per SVM. The allowed values for this parameter are 1 through 10.

A number of optional filter parameters enable you to customize the security trace filter so that you can narrow down the results produced by the security trace:

<table>
<thead>
<tr>
<th>Filter parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-client-ip IP_Address</td>
<td>This filter specifies the IP address from which the user is accessing the SVM.</td>
</tr>
<tr>
<td>-path path</td>
<td>This filter specifies the path on which to apply the permission trace filter. The value for -path can use either of the following formats:</td>
</tr>
<tr>
<td></td>
<td>• The complete path, starting from the root of the share</td>
</tr>
<tr>
<td></td>
<td>• A partial path, relative to the root of the share</td>
</tr>
<tr>
<td></td>
<td>You must use NFS style directory separators in the path value.</td>
</tr>
<tr>
<td>-windows-name win_user_name or -unix-name unix_user_name</td>
<td>You can specify either the Windows user name or UNIX user name whose access requests you want to trace. The user name variable is case insensitive. You cannot specify both a Windows user name and a UNIX user name in the same filter.</td>
</tr>
<tr>
<td>Note: Even though you can only trace SMB access events, the mapped UNIX user and the mapped UNIX users' groups might be used when performing access checks on mixed or UNIX security-style data.</td>
<td></td>
</tr>
<tr>
<td>-trace-allow {yes</td>
<td>no}</td>
</tr>
<tr>
<td>-enabled {enabled</td>
<td>disabled}</td>
</tr>
<tr>
<td>-time-enabled integer</td>
<td>You can specify a timeout for the filter, after which it is disabled.</td>
</tr>
</tbody>
</table>
Steps

1. Create a security trace filter:

   `vserver security trace filter create -vserver vserver_name -index index_number filter_parameters`

   **Example**

   `filter_parameters` is a list of optional filter parameters.

   For more information, see the man pages for the command.

2. Verify the security trace filter entry:

   `vserver security trace filter show -vserver vserver_name -index index_number`

   **Examples**

   The following command creates a security trace filter for any user accessing a file with a share path `\server\share1\dir1\dir2\file.txt` from the IP address 10.10.10.7. The filter uses a complete path for the `-path` option. The client's IP address used to access data is 10.10.10.7. The filter times out after 30 minutes:

   ```
   cluster1::> vserver security trace filter create -vserver vs1 -index 1 -path /dir1/dir2/file.txt -time-enabled 30 -client-ip 10.10.10.7
   cluster1::> vserver security trace filter show -index 1
   Vserver  Index   Client-IP            Path            Trace-Allow  Windows-Name
   -------- -----  -----------  ----------------------   -----------  -------------
   vs1        1    10.10.10.7   /dir1/dir2/file.txt          no       -
   ```

   The following command creates a security trace filter using a relative path for the `-path` option. The filter traces access for a Windows user named "joe". Joe is accessing a file with a share path `\server\share1\dir1\dir2\file.txt`. The filter traces allow and deny events:

   ```
   cluster1::> vserver security trace filter create -vserver vs1 -index 2 -path /dir1/dir2/file.txt -trace-allow yes -windows-name mydomain\joe
   cluster1::> vserver security trace filter show -vserver vs1 -index 2
   Vserver: vs1
   Filter Index: 2
   Client IP Address to Match: -
   Path: /dir1/dir2/file.txt
   Windows User Name: mydomain\joe
   UNIX User Name: -
   Trace Allow Events: yes
   Filter Enabled: enabled
   Minutes Filter is Enabled: 60
   ```

**Displaying information about security trace filters**

You can display information about security trace filters configured on your Storage Virtual Machine (SVM). This enables you to see which types of access events each filter traces.

**Step**

1. Display information about security trace filter entries by using the `vserver security trace filter show` command.

   For more information about using this command, see the man pages.

   **Examples**

   The following command displays information about all security trace filters on SVM vs1:
### Displaying security trace results

You can display the security trace results generated for file operations that match security trace filters. You can use the results to validate your file access security configuration or to troubleshoot SMB file access issues.

#### Before you begin

An enabled security trace filter must exist and operations must have been performed from an SMB client that matches the security trace filter to generate security trace results.

#### About this task

You can display a summary of all security trace results, or you can customize what information is displayed in the output by specifying optional parameters. This can be helpful when the security trace results contain a large number of records.

If you do not specify any of the optional parameters, the following is displayed:

- Storage Virtual Machine (SVM) name
- Node name
- Security trace index number
- Security style
- Path
- Reason
- User name

The user name displayed depends on how the trace filter is configured:

<table>
<thead>
<tr>
<th>If the filter is configured...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>With a UNIX user name</td>
<td>The security trace result displays the UNIX user name.</td>
</tr>
<tr>
<td>With a Windows user name</td>
<td>The security trace result displays the Windows user name.</td>
</tr>
<tr>
<td>Without a user name</td>
<td>The security trace result displays the Windows user name.</td>
</tr>
</tbody>
</table>

You can customize the output by using optional parameters. Some of the optional parameters that you can use to narrow the results returned in the command output include the following:

<table>
<thead>
<tr>
<th>Optional parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-fields field_name,...</td>
<td>Displays output on the fields you choose. You can use this parameter either alone or in combination with other optional parameters.</td>
</tr>
<tr>
<td>-instance</td>
<td>Displays detailed information about security trace events. Use this parameter with other optional parameters to display detailed information about specific filter results.</td>
</tr>
<tr>
<td>-node node_name</td>
<td>Displays information only about events on the specified node.</td>
</tr>
<tr>
<td>-vserver vserver_name</td>
<td>Displays information only about events on the specified SVM.</td>
</tr>
<tr>
<td>Optional parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>-index integer</td>
<td>Displays information about the events that occurred as a result of the filter corresponding to the specified index number.</td>
</tr>
<tr>
<td>-client-ip IP_address</td>
<td>Displays information about the events that occurred as a result of file access from the specified client IP address.</td>
</tr>
<tr>
<td>-path path</td>
<td>Displays information about the events that occurred as a result of file access to the specified path.</td>
</tr>
<tr>
<td>-user-name user_name</td>
<td>Displays information about the events that occurred as a result of file access by the specified Windows or UNIX user.</td>
</tr>
<tr>
<td>-security-style security_style</td>
<td>Displays information about the events that occurred on file systems with the specified security style.</td>
</tr>
</tbody>
</table>

See the man page for information about other optional parameters that you can use with the command.

**Step**

1. Display security trace filter results by using the `vserver security trace trace-result show` command.

**Example**

```
vserver security trace trace-result show -user-name domain\user
```

<table>
<thead>
<tr>
<th>Vserver: vs1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>node1</td>
</tr>
<tr>
<td>node1</td>
</tr>
</tbody>
</table>

**Related concepts**

*How to interpret security trace results* on page 292

**Modifying security trace filters**

If you want to change the optional filter parameters used to determine which access events are traced, you can modify existing security trace filters.

**About this task**

You must identify which security trace filter you want to modify by specifying the Storage Virtual Machine (SVM) name on which the filter is applied and the index number of the filter. You can modify all the optional filter parameters.

**Steps**

1. Modify a security trace filter:

```
vserver security trace filter modify -vserver vserver_name -index index_number filter_parameters
```

   - `vserver_name` is the name of the SVM on which you want to apply a security trace filter.
• `index_number` is the index number that you want to apply to the filter. The allowed values for this parameter are 1 through 10.

• `filter_parameters` is a list of optional filter parameters.

2. Verify the security trace filter entry:

   ```
vserver security trace filter show -vserver vserver_name -index index_number
   ```

Example

The following command modifies the security trace filter with the index number 1. The filter traces events for any user accessing a file with a share path `\server\share1\dir1\dir2\file.txt` from any IP address. The filter uses a complete path for the `-path` option. The filter traces allow and deny events:

```
cluster1::> vserver security trace filter modify -vserver vs1 -index 1 -path /dir1/dir2/file.txt -trace-allow yes
cluster1::> vserver security trace filter show -vserver vs1 -index 1
Vserver: vs1
Filter Index: 1
Client IP Address to Match: -
Path: /dir1/dir2/file.txt
Windows User Name: -
UNIX User Name: -
Trace Allow Events: yes
Filter Enabled: enabled
Minutes Filter is Enabled: 60
```

Deleting security trace filters

When you no longer need a security trace filter entry, you can delete it. Because you can have a maximum of 10 security trace filters per Storage Virtual Machine (SVM), deleting unneeded filters enables you to create new filters if you have reached the maximum.

About this task

To uniquely identify the security trace filter that you want to delete, you must specify the following:

• The name of the SVM to which the trace filter is applied

• The filter index number of the trace filter

Steps

1. Identify the filter index number of the security trace filter entry you want to delete:

   ```
vserver security trace filter show -vserver vserver_name
   ```

   **Example**

   ```
vserver security trace filter show -vserver vs1
   ```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Index</th>
<th>Client-IP</th>
<th>Path</th>
<th>Trace-Allow</th>
<th>Windows-Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>1</td>
<td>-</td>
<td>/dir1/dir2/file.txt</td>
<td>yes</td>
<td>-</td>
</tr>
<tr>
<td>vs1</td>
<td>2</td>
<td>-</td>
<td>/dir3/dir4/</td>
<td>no</td>
<td>mydomain\joe</td>
</tr>
</tbody>
</table>

2. Using the filter index number information from the previous step, delete the filter entry:

   ```
vserver security trace filter delete -vserver vserver_name -index index_number
   ```
Example
```
vserver security trace filter delete -vserver vs1 -index 1
```

3. Verify that the security trace filter entry is deleted:
```
vserver security trace filter show -vserver vserver_name
```

Example
```
vserver security trace filter show -vserver vs1
```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Index</th>
<th>Client-IP</th>
<th>Path</th>
<th>Trace-Allow</th>
<th>Windows-Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>2</td>
<td>-</td>
<td>/dir3/dir4/</td>
<td>no</td>
<td>mydomain\joe</td>
</tr>
</tbody>
</table>

Deleting security trace records

After you finish using a filter trace record to verify file access security or to troubleshoot SMB client access issues, you can delete the security trace record from the security trace log.

About this task

Before you can delete a security trace record, you must know the record's sequence number.

**Note:** Each Storage Virtual Machine (SVM) can store a maximum of 128 trace records. If the maximum is reached on the SVM, the oldest trace records are automatically deleted as new ones are added. If you do not want to manually delete trace records on this SVM, you can let Data ONTAP automatically delete the oldest trace results after the maximum is reached to make room for new results.

Steps

1. Identify the sequence number of the record you want to delete:
```
vserver security trace trace-result show -vserver vserver_name -instance
```

2. Delete the security trace record:
```
vserver security trace trace-result delete -node node_name -vserver vserver_name -seqnum integer
```

Example
```
vserver security trace trace-result delete -vserver vs1 -node node1 -seqnum 999
```

- `-node node_name` is the name of the cluster node on which the permission tracing event that you want to delete occurred.
  This is a required parameter.

- `-vserver vserver_name` is the name of the SVM on which the permission tracing event that you want to delete occurred.
  This is a required parameter.

- `-seqnum integer` is the sequence number of the log event that you want to delete.
  This is a required parameter.
Deleting all security trace records

If you do not want to keep any of the existing security trace records, you can delete all of the records on a node with a single command.

Step

1. Delete all security trace records:

   ```
   vserver security trace trace-result delete -node node_name -vserver vserver_name *
   ```

   - `-node node_name` is the name of the cluster node on which the permission tracing event that you want to delete occurred.
   - `-vserver vserver_name` is the name of the Storage Virtual Machine (SVM) on which the permission tracing event that you want to delete occurred.

How to interpret security trace results

Security trace results provide the reason that a request was allowed or denied. Output displays the result as a combination of the reason for allowing or denying access and the location within the access checking pathway where access is either allowed or denied. You can use the results to isolate and identify why actions are or are not allowed.

Finding information about the lists of result types and filter details

You can find the lists of result types and filter details that can be included in the security trace results in the man pages for the `vserver security trace trace-result show` command.

Example of output from the `Reason` field in an `Allow` result type

The following is an example of the output from the `Reason` field that appears in the trace results log in an `Allow` result type:

```
Access is allowed because CIFS implicit permission grants requested access while opening existing file or directory.
```

Example of output from the `Reason` field in an `Allow` result type

The following is an example of the output from the `Reason` field that appears in the trace results log in a `Deny` result type:

```
Access is denied. The requested permissions are not granted by the ACE while checking for child-delete access on the parent.
```

Example of output from the `Filter details` field

The following is an example of the output from the `Filter details` field in the trace results log, which list the effective security style of the file system containing files and folders that match the filter criteria:

```
Security Style: MIXED and ACL
```

Related tasks

`Performing security traces` on page 285
Configuring the metadata cache for SMB shares

Metadata caching enables file attribute caching on SMB 1.0 clients to provide faster access to file and folder attributes. You can enable or disable attribute caching on a per-share basis. You can also configure the time-to-live for cached entries if metadata caching is enabled. Configuring metadata caching is not necessary if clients are connecting to shares over SMB 2.x or SMB 3.0.

How SMB metadata caching works

When enabled, the SMB metadata cache stores path and file attribute data for a limited amount of time. This can improve SMB performance for SMB 1.0 clients with common workloads.

For certain tasks, SMB creates a significant amount of traffic that can include multiple identical queries for path and file metadata. You can reduce the number of redundant queries and improve performance for SMB 1.0 clients by using SMB metadata caching to fetch information from the cache instead.

Attention: While unlikely, it is possible that the metadata cache might serve stale information to SMB 1.0 clients. If your environment cannot afford this risk, you should not enable this feature.

Enabling the SMB metadata cache

You can improve SMB performance for SMB 1.0 clients by enabling the SMB metadata cache. By default, SMB metadata caching is disabled.

Step

1. Perform the desired action:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SMB metadata caching when you create a share</td>
<td><code>vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties attributecache</code></td>
</tr>
<tr>
<td>Enable SMB metadata caching on an existing share</td>
<td><code>vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties attributecache</code></td>
</tr>
</tbody>
</table>

Related tasks

- Configuring the lifetime of SMB metadata cache entries on page 293
- Creating an SMB share on a CIFS server on page 177
- Adding or removing share properties on an existing SMB share on page 183

Configuring the lifetime of SMB metadata cache entries

You can configure the lifetime of SMB metadata cache entries to optimize the SMB metadata cache performance in your environment. The default is 10 seconds.

Before you begin

You must have enabled the SMB metadata cache feature. If SMB metadata caching is not enabled, the SMB cache TTL setting is not used.
Step

1. Perform the desired action:

<table>
<thead>
<tr>
<th>If you want to configure the lifetime of SMB metadata cache entries when you...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a share</td>
<td><code>vserver cifs share -create -vserver vserver_name -share-name share_name -path path -attribute-cache-ttl [integer][integer][integer]</code></td>
</tr>
<tr>
<td>Modify an existing share</td>
<td><code>vserver cifs share -modify -vserver vserver_name -share-name share_name -attribute-cache-ttl [integer][integer][integer]</code></td>
</tr>
</tbody>
</table>

You can specify additional share configuration options and properties when you create or modify shares. See the man pages for more information.

Managing file locks

You can display information about the current locks for a Storage Virtual Machine (SVM) as a first step to determining why a client cannot access a volume or file. You can use this information if you need to break file locks.

For information about how file locks affect Infinite Volumes, see the *Clustered Data ONTAP Infinite Volumes Management Guide*.

About file locking between protocols

File locking is a method used by client applications to prevent a user from accessing a file previously opened by another user. How Data ONTAP locks files depends on the protocol of the client.

If the client is an NFS client, locks are advisory; if the client is an SMB client, locks are mandatory.

Because of differences between the NFS and SMB file locks, an NFS client might fail to access a file previously opened by an SMB application.

The following occurs when an NFS client attempts to access a file locked by an SMB application:

- In mixed or NTFS volumes, file manipulation operations such as `rm`, `rmdir`, and `mv` can cause the NFS application to fail.
- NFS read and write operations are denied by SMB deny-read and deny-write open modes, respectively.
- NFS write operations fail when the written range of the file is locked with an exclusive SMB bytelock.

In UNIX security-style volumes, NFS unlink and rename operations ignore SMB lock state and allow access to the file. All other NFS operations on UNIX security-style volumes honor SMB lock state.

How Data ONTAP treats read-only bits

The read-only bit is a binary digit, which holds a value of 0 or 1, that is set on a file-by-file basis to reflect whether a file is writable (disabled) or read-only (enabled).

SMB clients that use MS-DOS and Windows can set a per-file read-only bit. NFS clients do not set a per-file read-only bit because NFS clients do not have any protocol operations that use a per-file read-only bit.

Data ONTAP can set a read-only bit on a file when an SMB client that uses MS-DOS or Windows creates that file. Data ONTAP can also set a read-only bit when a file is shared between NFS clients.
and SMB clients. Some software, when used by NFS clients and SMB clients, requires the read-only bit to be enabled.

For Data ONTAP to keep the appropriate read and write permissions on a file shared between NFS clients and SMB clients, it treats the read-only bit according to the following rules:

- NFS treats any file with the read-only bit enabled as if it has no write permission bits enabled.
- If an NFS client disables all write permission bits and at least one of those bits had previously been enabled, Data ONTAP enables the read-only bit for that file.
- If an NFS client enables any write permission bit, Data ONTAP disables the read-only bit for that file.
- If the read-only bit for a file is enabled and an NFS client attempts to discover permissions for the file, the permission bits for the file are not sent to the NFS client; instead, Data ONTAP sends the permission bits to the NFS client with the write permission bits masked.
- If the read-only bit for a file is enabled and an SMB client disables the read-only bit, Data ONTAP enables the owner’s write permission bit for the file.
- Files with the read-only bit enabled are writable only by root.

Note: Changes to file permissions take effect immediately on SMB clients, but might not take effect immediately on NFS clients if the NFS client enables attribute caching.

How Data ONTAP differs from Windows on handling locks on share path components
Unlike Windows, Data ONTAP does not lock each component of the path to an open file while the file is open. This behavior also affects SMB share paths.

Because Data ONTAP does not lock each component of the path, it is possible to rename a path component above the open file or share, which can cause problems for certain applications, or can cause the share path in the SMB configuration to be invalid. This can cause the share to be inaccessible.

To avoid issues caused by renaming path components, you can apply security settings that prevent users or applications from renaming critical directories.

Displaying information about locks
You can display information about the current file locks, including what types of locks are held and what the lock state is, details about byte-range locks, sharelock modes, delegation locks, and opportunistic locks, and whether locks are opened with durable or persistent handles.

About this task
The client IP address cannot be displayed for locks established through NFSv4 or NFSv4.1.

By default, the command displays information about all locks. You can use command parameters to display information about locks for a specific Storage Virtual Machine (SVM) or to filter the command's output by other criteria. If you do not specify any parameter, the command displays the following information:

- SVM name
- Volume name of the FlexVol volume or the name of the namespace constituent for the Infinite Volume
- Path of the locked object
- Logical interface name
• Protocol by which the lock was established
• Type of lock
• Client

The `vserver locks show` command displays information about four types of locks:

• Byte-range locks, which lock only a portion of a file.
• Share locks, which lock open files.
• Opportunistic locks, which control client-side caching over SMB.
• Delegations, which control client-side caching over NFSv4.x.

By specifying optional parameters, you can determine important information about each of these lock types. See the man page for the command for more information.

**Step**

1. Display information about locks by using the `vserver locks show` command.

**Examples**

The following example displays summary information for an NFSv4 lock on a file with the path `/vol1/file1`. The sharelock access mode is write-deny_none, and the lock was granted with write delegation:

```
cluster1::> vserver locks show
Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- ----------- -------
vol1    /vol1/file1               lif1        nfsv4     share-level -
Sharelock Mode: write-deny_none
delegation -
Delegation Type: write
```

The following example displays detailed oplock and sharelock information about the SMB lock on a file with the path `/data2/data2_2/intro.pptx`. A durable handle is granted on the file with a share lock access mode of write-deny_none to a client with an IP address of 10.3.1.3. A lease oplock is granted with a batch oplock level:

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx
Vserver: vs1
Volume: data2_2
Logical Interface: lif2
Object Path: /data2/data2_2/intro.pptx
Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
Lock Protocol: cifs
Lock Type: share-level
Node Holding Lock State: node3
Lock State: granted
Bytelock Starting Offset: -
Number of Bytes Locked: -
Bytelock is Mandatory: -
Bytelock is Exclusive: -
Bytelock is Superlock: -
Bytelock is Soft: -
Oplock Level: -
Shared Lock Access Mode: write-deny_none
Shared Lock is Soft: false
Delegation Type: -
Client Address: 10.3.1.3
SMB Open Type: durable
SMB Connect State: connected
SMB Expiration Time (Secs): -
SMB Open Group ID: 78a90c59d45ae211998100059a3c7a00a07f70da0f8fffcdf445b030000000
Vserver: vs1
Volume: data2_2
Logical Interface: lif2
```
Breaking locks

When file locks are preventing client access to files, you can display information about currently held locks, and then break specific locks. Examples of scenarios in which you might need to break locks include debugging applications.

About this task

The `vserver locks break` command is available only at the advanced privilege level and higher. The man page for the command contains detailed information.

Steps

1. To find the information you need to break a lock, use the `vserver locks show` command.
   The man page for the command contains detailed information.
2. Set the privilege level to advanced:
   `set -privilege advanced`
3. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want to break a lock by specifying...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>The SVM name, volume name, LIF name, and file path</td>
<td><code>vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif</code></td>
</tr>
<tr>
<td>The lock ID</td>
<td><code>vserver locks break -lockid UUID</code></td>
</tr>
</tbody>
</table>

-`vserver vserver_name` specifies the SVM name.
-`-volume volume_name` specifies the volume name of the FlexVol volume or the name of the namespace constituent for the Infinite Volume.
-`-path path` specifies the path.
-`-lif lif` specifies the logical interface.
-`-lockid UUID` specifies the universally unique identifier for the lock.

4. Return to the admin privilege level:
   `set -privilege admin`
Monitoring SMB activity

You can monitor SMB activity by displaying information about SMB sessions and open files. You can also display information about SMB statistics.

Displaying SMB session information

You can display information about established SMB sessions, including the SMB connection and session ID and the IP address of the workstation using the session. You can display information about the session’s SMB protocol version and continuously available protection level, which helps you identify whether the session supports nondisruptive operations.

About this task

You can display information for all sessions on your Storage Virtual Machine (SVM) in summary form. However, in many cases, the amount of output returned is large. You can customize what information is displayed in the output by specifying optional parameters:

- You can use the optional -fields parameter to display output on the fields you choose. You can enter -fields ? to determine what fields you can use.
- You can use the -instance parameter to display detailed information about established SMB sessions.
- You can use the -fields parameter or the -instance parameter either alone or in combination with other optional parameters.

Step

1. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want to display SMB session information for established sessions...</th>
<th>Enter the following command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>For all sessions on the SVM in summary form</td>
<td><code>vserver cifs session show -vserver vserver_name</code></td>
</tr>
<tr>
<td>On a specified connection ID</td>
<td><code>vserver cifs session show -vserver vserver_name -connection-id integer</code></td>
</tr>
<tr>
<td>From a specified workstation IP address</td>
<td><code>vserver cifs session show -vserver vserver_name -address workstation_IP_address</code></td>
</tr>
<tr>
<td>On the specified LIF IP address</td>
<td><code>vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address</code></td>
</tr>
<tr>
<td>On a specified node</td>
<td>`vserver cifs session show -vserver vserver_name -node (node_name</td>
</tr>
<tr>
<td>From a specified Windows user</td>
<td><code>vserver cifs session show -vserver vserver_name -windows-user user_name</code></td>
</tr>
</tbody>
</table>

The format for `user_name` is `[domain]\user.`
<table>
<thead>
<tr>
<th>Session Information</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>For established sessions...</td>
<td>vserver cifs session show -vserver vserver_name -auth-mechanism authentication_mechanism</td>
</tr>
<tr>
<td>With a specified</td>
<td></td>
</tr>
<tr>
<td>authentication mechanism</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The value for -auth-mechanism can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• NTLMv1</td>
</tr>
<tr>
<td></td>
<td>• NTLMv2</td>
</tr>
<tr>
<td></td>
<td>• Kerberos</td>
</tr>
<tr>
<td></td>
<td>• Anonymous</td>
</tr>
<tr>
<td>With the specified protocol</td>
<td>vserver cifs session show -vserver vserver_name -protocol-version protocol_version</td>
</tr>
<tr>
<td>version</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The value for -protocol-version can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• SMB1</td>
</tr>
<tr>
<td></td>
<td>• SMB2</td>
</tr>
<tr>
<td></td>
<td>• SMB2_1</td>
</tr>
<tr>
<td></td>
<td>• SMB3</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Continuously available protection is available only on SMB 3.0 sessions. To see continuously available protection status on all qualifying sessions, specify this parameter with the value set to SMB3.</td>
</tr>
<tr>
<td>With the specified level of</td>
<td>vserver cifs session show -vserver vserver_name -continuously-available continuously_available_protection_level</td>
</tr>
<tr>
<td>continuously available</td>
<td></td>
</tr>
<tr>
<td>protection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The value for -continuously-available can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• No</td>
</tr>
<tr>
<td></td>
<td>• Yes</td>
</tr>
<tr>
<td></td>
<td>• Partial</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If the continuously available status is Partial, this means that the session contains at least one open continuously available file, but the session has some files that are not open with continuously available protection. You can use the vserver cifs sessions file show command to determine which files on the established session are not open with continuously available protection.</td>
</tr>
<tr>
<td>With the specified SMB</td>
<td>vserver cifs session show -vserver vserver_name -is-session-signed (true</td>
</tr>
<tr>
<td>signing session status</td>
<td></td>
</tr>
</tbody>
</table>

### Examples

The following command displays session information on SVM sessions vs1 established from a workstation with the IP address of 10.1.1.1:
The following command displays detailed session information on sessions with continuously available protection on SVM vs1. The connection was made by using the domain computer-machine account.

```bash
cluster1::> vserver cifs session show -instance -continuously-available Yes
```

Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation IP address: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\SERVER1$
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: Yes
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted

The following command displays session information on sessions using SMB 3.0 on SVM vs1. The user connected to this share from an SMB 3.0 capable client by using the LIF IP address; therefore, the authentication mechanism defaulted to NTLMv2. The connection must be made using Kerberos authentication to connect with continuously available protection.

```bash
cluster1::> vserver cifs session show -instance -protocol-version SMB3
```

Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 3151272607
Incoming Data LIF IP Address: 10.2.1.2
Workstation IP address: 10.1.1.3
Authentication Mechanism: NTLMv2
Windows User: DOMAIN\administrator
UNIX User: pcuser
Open Shares: 1
Open Files: 0
Open Other: 0
Connected Time: 6m 22s
Idle Time: 5m 42s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted

### Related tasks

* Displaying information about open SMB files on page 301*
Displaying information about open SMB files

You can display information about open SMB files, including the SMB connection and session ID, the hosting volume, the share name, and the share path. You can display information about a file’s continuously available protection level, which is helpful in determining whether an open file is in a state that supports nondisruptive operations.

About this task

You can display information about open files on an established SMB session. The displayed information is useful when you need to determine SMB session information for particular files within an SMB session.

For example, if you have an SMB session where some of the open files are open with continuously available protection and some are not open with continuously available protection (the value for the -continuously-available field in vserver cifs session show command output is Partial), you can determine which files are not continuously available by using this command.

You can display information for all open files on established SMB sessions on Storage Virtual Machines (SVMs) in summary form by using the vserver cifs session file show command without any optional parameters. However, in many cases, the amount of output returned is large. You can customize what information is displayed in the output by specifying optional parameters. This can be helpful when you want to view information for only a small subset of open files.

- You can use the optional -fields parameter to display output on the fields you choose. You can use this parameter either alone or in combination with other optional parameters.
- You can use the -instance parameter to display detailed information about open SMB files. You can use this parameter either alone or in combination with other optional parameters.

Step

1. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want to display open SMB files...</th>
<th>Enter the following command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>On the SVM in summary form</td>
<td>vserver cifs session file show -vserver vserver_name</td>
</tr>
<tr>
<td>On a specified node</td>
<td>vserver cifs session file show -vserver vserver_name -node {node_name</td>
</tr>
<tr>
<td>On a specified file ID</td>
<td>vserver cifs session file show -vserver vserver_name -file-id integer</td>
</tr>
<tr>
<td>On a specified SMB connection ID</td>
<td>vserver cifs session file show -vserver vserver_name -connection-id integer</td>
</tr>
<tr>
<td>On a specified SMB session ID</td>
<td>vserver cifs session file show -vserver vserver_name -session-id integer</td>
</tr>
<tr>
<td>On the specified hosting aggregate</td>
<td>vserver cifs session file show -vserver vserver_name -hosting-aggregate aggregate_name</td>
</tr>
</tbody>
</table>
If you want to display open SMB files...

Enter the following command...

On the specified volume

vserver cifs session file show -vserver
vserver_name -hosting-volume volume_name

On the specified SMB share

vserver cifs session file show -vserver
vserver_name -share share_name

On the specified SMB path

vserver cifs session file show -vserver
vserver_name -path path

With the specified level of continuously available protection

vserver cifs session file show -vserver
vserver_name -continuously-available
continuously_available_status

The value for -continuously-available can be one of the following:

• No

• Yes

Note: If the continuously available status is No, this means that these open files are not capable of nondisruptively recovering from takeover and giveback. They also cannot recover from general aggregate relocation between partners in a high-availability relationship.

With the specified reconnected state

vserver cifs session file show -vserver
vserver_name -reconnected reconnected_state

The value for -reconnected can be one of the following:

• No

• Yes

Note: If the reconnected state is No, the open file is not reconnected after a disconnection event. This can mean that the file was never disconnected, or that the file was disconnected and is not successfully reconnected. If the reconnected state is Yes, this means that the open file is successfully reconnected after a disconnection event.

There are additional optional parameters that you can use to refine the output results. See the man page for more information.

Examples

The following example displays information about open files on SVM vs1:

cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting               Continuously
ID      Type      Mode Volume    Share       Available
------- --------- ---- --------- ----------- ------------
41      Regular   r    data      data        Yes
Path: \mytest.rtf

The following example displays detailed information about open SMB files with file ID 82 on SVM vs1:
Related tasks

*Displaying SMB session information* on page 298

Related information

*Clustered Data ONTAP 8.3.1 man page: vserver cifs session file show - Display opened CIFS files
Clustered Data ONTAP 8.3.1 man page: vserver cifs session file close - Close an open CIFS file*

Determining which statistics objects and counters are available

Before you can obtain information about CIFS, SMB, auditing, and BranchCache hash statistics and monitor performance, you must know which objects and counters are available from which you can obtain data.

**Steps**

1. Set the privilege level to advanced:
   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want to determine...</th>
<th>Enter...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Which objects are available</td>
<td><code>statistics catalog object show</code></td>
</tr>
<tr>
<td>Specific objects that are</td>
<td><code>statistics catalog object show -object</code></td>
</tr>
<tr>
<td>available</td>
<td><code>object_name</code></td>
</tr>
<tr>
<td>Which counters are available</td>
<td><code>statistics catalog counter show -object</code></td>
</tr>
<tr>
<td></td>
<td><code>object_name</code></td>
</tr>
</tbody>
</table>

   See the man pages for more information about which objects and counters are available.

3. Return to the admin privilege level:
   ```
   set -privilege admin
   ```

**Examples**

The following command displays descriptions of selected statistic objects related to CIFS and SMB access in the cluster as seen at the advanced privilege level:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.
```
Do you want to continue? {y|n}: y

cluster1::> statistics catalog object show -object audit
audit_ng                  CM object for exporting audit_ng performance counters

cluster1::> statistics catalog object show -object cifs
cifs                      The CIFS object reports activity of the Common Internet File System (CIFS) protocol that evolved from the Server Message Block (SMB) application layer network protocol to connect PCs to Network Attached Storage devices (NAS). This object reports activity for both SMB and SMB2 revisions of the CIFS protocol. For information related only to SMB, see the 'smb1' object. For information related only to SMB2, see the 'smb2' object.

The following command displays information about some of the counters for the **cifs** object as seen at the advanced privilege level:

**Note:** This example does not display all of the available counters for the **cifs** object; output is truncated.

```text
cluster1::> set -privilege admin
Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
cluster1::> set -privilege advanced
```

```
cluster1::> statistics catalog counter show -object cifs
Object: cifs
Counter                  Description                                                                                     
--------------------------------------------------------------------------------------------------------
auth_reject_too_many     Number of active searches over SMB and SMB2 Authentication refused after too many requests were made in rapid succession
avg_directory_depth      Average number of directories crossed by SMB and SMB2 path-based commands
avg_junction_depth       Average number of junctions crossed by SMB and SMB2 path-based commands
branchcache_hash_fetch_fail Total number of times a request to fetch hash data failed. These are failures when attempting to read existing hash data. It does not include attempts to fetch hash data that has not yet been generated.
branchcache_hash_fetch_ok Total number of times a request to fetch hash data succeeded.
branchcache_hash_sent_bytes Total number of bytes sent to clients requesting hashes.
branchcache_missing_hash_bytes Total number of bytes of data that had to be
```
Related tasks

*Displaying statistics* on page 305

Related information

*Clustered Data ONTAP 8.3.1 man page: statistics catalog object show - Display the list of objects*

*Clustered Data ONTAP 8.3.1 man page: statistics catalog counter show - Display the list of counters in an object*

### Displaying statistics

You can display various statistics, including statistics about CIFS and SMB, auditing, and BranchCache hashes, to monitor performance and diagnose issues.

#### Before you begin

You must have collected data samples by using the `statistics start` and optional `statistics stop` commands before you can display information about objects. For more information about these commands, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

#### Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want to display statistics for...</th>
<th>Enter...</th>
</tr>
</thead>
<tbody>
<tr>
<td>All versions of SMB</td>
<td><code>statistics show -object cifs</code></td>
</tr>
<tr>
<td>SMB 1.0</td>
<td><code>statistics show -object smb1</code></td>
</tr>
<tr>
<td>SMB 2.x and SMB 3.0</td>
<td><code>statistics show -object smb2</code></td>
</tr>
<tr>
<td>CIFS subsystem of the node</td>
<td><code>statistics show -object nblade_cifs</code></td>
</tr>
<tr>
<td>Multiprotocol audit</td>
<td><code>statistics show -object audit_ng</code></td>
</tr>
<tr>
<td>BranchCache hash service</td>
<td><code>statistics show -object hashd</code></td>
</tr>
</tbody>
</table>

   See the man page for each command for more information.

3. Return to the admin privilege level:

   ```
   set -privilege admin
   ```
Related tasks

Determining which statistics objects and counters are available on page 303
Monitoring SMB signed session statistics on page 90
Displaying BranchCache statistics on page 351
Using statistics to monitor automatic node referral activity on page 368
Using statistics to monitor Hyper-V and SQL Server over SMB activity on page 407

Related information

Clustered Data ONTAP 8.3.1 man page: statistics show - Display performance data for a time interval
Deploying CIFS client-based services

You can deploy a number of CIFS client-based services, such as accessing files in Snapshot copies using the Previous Versions Windows Properties tab; and configuring offline folders, roaming profiles, and folder redirection.

Using offline files to allow caching of files for offline use

Data ONTAP supports the Microsoft Offline Files feature, or client-side caching, which allows files to be cached on the local host for offline use. Users can use the offline files functionality to continue working on files even when they are disconnected from the network.

You can specify whether Windows user documents and programs are automatically cached on a share or whether the files must be manually selected for caching. Manual caching is enabled by default for new shares. The files that are made available offline are synchronized to the Windows client's local disk. Synchronization occurs when network connectivity to a specific storage system share is restored.

Because offline files and folders retain the same access permissions as the version of the files and folders saved on the CIFS server, the user must have sufficient permissions on the files and folders saved on the CIFS server to perform actions on the offline files and folders.

When the user and someone else on the network make changes to the same file, the user can save the local version of the file to the network, keep the other version, or save both. If the user keeps both versions, a new file with the local user's changes is saved locally and the cached file is overwritten with changes from the version of the file saved on the CIFS server.

You can configure offline files on a share-by-share basis by using share configuration settings. You can choose one of the four offline folder configurations when you create or modify shares:

- **No caching**
  Enables client-side caching for the share. Files and folders are not automatically cached locally on clients and users cannot choose to cache files or folders locally.

- **Manual caching**
  Enables manual selection of files to be cached on the share. This is the default setting. By default, no files or folders are cached on the local client. Users can choose which files and folders they want to cache locally for offline use.

- **Automatic document caching**
  Enables user documents to be automatically cached on the share. Only files and folders that are accessed are cached locally.

- **Automatic program caching**
  Enables programs and user documents to be automatically cached on the share. Only files, folders, and programs that are accessed are cached locally. Additionally, this setting allows the client to run locally cached executables even when connected to the network.

For more information about configuring offline files on Windows servers and clients, consult the Microsoft TechNet Library.

Related concepts

*Using roaming profiles to store user profiles centrally on a CIFS server associated with the SVM* on page 311

*Using folder redirection to store data on a CIFS server* on page 312
Related information


Requirements for using offline files

Before you can use the Microsoft Offline Files feature with your CIFS server, you need to know which versions of Data ONTAP and SMB and which Windows clients support the feature.

Data ONTAP version requirements

Data ONTAP 8.2 and later releases support offline files.

SMB protocol version requirements

For Storage Virtual Machine (SVM) with FlexVol volumes, Data ONTAP supports offline files on all versions of SMB.

For SVM with Infinite Volume, Data ONTAP supports offline files on SMB 1.0.

Windows client requirements

The Windows client must support the offline files.

For the latest information about which Windows clients supports the Offline Files feature, see the Interoperability Matrix at mysupport.netapp.com/matrix.

Considerations when deploying offline files

There are some important considerations you need to understand when you deploy offline files on home directory shares that have the `showsnapshot` share property set on home directories.

If the `showsnapshot` share property is set on a home directory share that has offline files configured, Windows clients cache all of the Snapshot copies under the `~snapshot` folder in the user’s home directory.

Windows clients cache all of the Snapshot copies under the home directory if one of more of the following is true:

- The user makes the home directory available offline from the client.
  The contents of the `~snapshot` folder in the home directory is included and made available offline.

- The user configures folder redirection to redirect a folder such as `My Documents` to the root of a home directory residing on the CIFS server share.
  Some Windows clients might automatically make the redirected folder available offline. If the folder is redirected to the root of the home directory, the `~snapshot` folder is included in the cached offline content.

**Note:** Offline file deployments where the `~snapshot` folder is included in offline files should be avoided. The Snapshot copies in the `~snapshot` folder contain all data on the volume at the point at which Data ONTAP created the Snapshot copy. Therefore, creating an offline copy of the `~snapshot` folder consumes significant local storage on the client, consumes network bandwidth during offline files synchronization, and increases the time it takes to synchronize offline files.
Configuring offline files support on SMB shares using the CLI

You can configure offline files support using the Data ONTAP CLI by specifying one of the four offline files setting when you create SMB shares or at any time by modifying existing SMB shares. Manual offline files support is the default setting.

About this task

When configuring offline files support, you can choose one of the following four offline files settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>Disallows Windows clients from caching any files on this share.</td>
</tr>
<tr>
<td>manual</td>
<td>Allows users on Windows clients to manually select files to be cached.</td>
</tr>
<tr>
<td>documents</td>
<td>Allows Windows clients to cache user documents that are used by the user for offline access.</td>
</tr>
<tr>
<td>programs</td>
<td>Allows Windows clients to cache programs that are used by the user for offline access. Clients can use the cached program files in offline mode even if the share is available.</td>
</tr>
</tbody>
</table>

You can choose only one offline file setting. If you modify an offline files setting on an existing SMB share, the new offline files setting replaces the original setting. Other existing SMB share configuration settings and share properties are not removed or replaced. They remain in effect until they are explicitly removed or changed.

Steps

1. Perform the appropriate action:

<table>
<thead>
<tr>
<th>If you want to configure offline files on...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>A new SMB share</td>
<td>vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none</td>
</tr>
<tr>
<td>An existing SMB share</td>
<td>vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none</td>
</tr>
</tbody>
</table>

2. Verify that the SMB share configuration is correct:

   vserver cifs share show -vserver vserver_name -share-name share_name -instance

Example

The following command creates an SMB share named “data1” with offline files set to documents:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name datal -path /datal -comment "Offline files" -offline-files documents
```

```
cluster1::> vserver cifs share show -vserver vs1 -share-name datal -instance
```

```
Vserver: vs1
Share: datal
CIFS Server NetBIOS Name: VS1
Path: /datal
```
The following command modifies an existing SMB share named “data1” by changing the offline files setting to `manual` and adding values for the file and directory mode creation mask:

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name data1 - offline-files manual -file-umask 644 -dir-umask 777
```

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data1 -instance
```

Related tasks

Creating an SMB share on a CIFS server on page 177

Adding or removing share properties on an existing SMB share on page 183

Configuring offline files support on SMB shares by using the Computer Management MMC

If you want to permit users to cache files locally for offline use, you can configure offline files support by using the Computer Management MMC (Microsoft Management Console).

Steps

1. To open the MMC on your Windows server, in Windows Explorer, right-click the icon for the local computer and select Manage.
2. On the left panel, select Computer Management.
3. Select Action > Connect to another computer.
   The Select Computer dialog box appears.
4. Type the name of the CIFS server or click Browse to locate the CIFS server.
If the name of CIFS server is the same as the Storage Virtual Machine (SVM) host name, type the SVM name. If the CIFS server name is different from the SVM host name, type the name of the CIFS server.

5. Click OK.

6. In the console tree, click System Tools > Shared Folders.

7. Click Shares.

8. In the results pane, right-click the share.

9. Click Properties.

   Properties for the share you selected are displayed.

10. In the General tab, click Offline Settings.

    The Offline Settings dialog box appears.

11. Configure the offline availability options as appropriate.

12. Click OK.

Using roaming profiles to store user profiles centrally on a CIFS server associated with the SVM

Data ONTAP supports storing Windows roaming profiles on a CIFS server associated with the Storage Virtual Machine (SVM). Configuring user roaming profiles provides advantages to the user such as automatic resource availability regardless of where the user logs in. Roaming profiles also simplify the administration and management of user profiles.

Roaming user profiles have the following advantages:

- Automatic resource availability
  A user's unique profile is automatically available when that user logs in to any computer on the network that is running Windows 8, Windows 7, Windows Vista, Windows 2000, or Windows XP. Users do not need to create a profile on each computer they use on a network.

- Simplified computer replacement
  Because all of the user's profile information is maintained separately on the network, a user's profile can be easily downloaded onto a new, replacement computer. When the user logs in to the new computer for the first time, the server copy of the user's profile is copied to the new computer.

Related concepts

- Using offline files to allow caching of files for offline use on page 307
- Using folder redirection to store data on a CIFS server on page 312

Requirements for using roaming profiles

Before you can use Microsoft's roaming profiles with your CIFS server, you need to know which versions of Data ONTAP and SMB and which Windows clients support the feature.

Data ONTAP version requirements

Data ONTAP 8.2 and later support roaming profiles.
SMB protocol version requirements
For Storage Virtual Machine (SVM) with FlexVol volumes, Data ONTAP supports roaming profiles on all versions of SMB.

For SVM with Infinite Volume, Data ONTAP supports roaming profiles on SMB 1.0.

Windows client requirements
Before a user can use the roaming profiles, the Windows client must support the feature.

For the latest information about which Windows clients support roaming profiles, see the Interoperability Matrix at mysupport.netapp.com/matrix.

Configuring roaming profiles
If you want to automatically make a user’s profile available when that user logs on to any computer on the network, you can configure roaming profiles through the Active Directory Users and Computers MMC snap-in. If you are configuring roaming profiles on Windows Server 2012, you can use the Active Directory Administration Center.

Steps
1. On the Windows server, open the Active Directory Users and Computers MMC (or the Active Directory Administration Center on Windows 2012 and later servers).
2. Locate the user for which you want to configure a roaming profile.
3. Right-click the user and click Properties.
4. On the Profile tab, enter the profile path to the share where you want to store the user's roaming profile, followed by %username%.
   
   For example, a profile path might be the following: \vs1.example.com\profiles\%username%. The first time a user logs in, %username% is replaced with the user's name.

   Note: In the path \vs1.example.com\profiles\%username%, profiles is the share name of a share on Storage Virtual Machine (SVM) vs1 that has Full Control rights for Everyone.

5. Click OK.

Using folder redirection to store data on a CIFS server
Data ONTAP supports Microsoft folder redirection, which enables users or administrators to redirect the path of a local folder to a location on the CIFS server. It appears as if redirected folders are stored on the local Windows client, even though the data is stored on an SMB share.

Folder redirection is intended mostly for organizations that have already deployed home directories, and that want to maintain compatibility with their existing home directory environment.

• Documents, Desktop, and Start Menu are examples of folders that you can redirect.
• Users can redirect folders from their Windows client.
• Administrators can centrally configure and manage folder redirection by configuring GPOs in Active Directory.
• If administrators have configured roaming profiles, folder redirection enables administrators to divide user data from profile data.
Administrators can use folder redirection and offline files together to redirect data storage for local folders to the CIFS server, while allowing users to cache the content locally.

**Related concepts**
- Using offline files to allow caching of files for offline use on page 307
- Using roaming profiles to store user profiles centrally on a CIFS server associated with the SVM on page 311

**Requirements for using folder redirection**

Before you can use Microsoft's folder redirection with your CIFS server, you need to know which versions of Data ONTAP and SMB and which Windows clients support the feature.

**Data ONTAP version requirements**

Clustered Data ONTAP 8.2 and later support Microsoft folder redirection.

**SMB protocol version requirements**

For Storage Virtual Machine (SVM) with FlexVol volumes, Data ONTAP supports Microsoft's folder redirection on all versions of SMB.

For SVM with Infinite Volume, Data ONTAP supports Microsoft's folder redirection on SMB 1.0.

**Windows client requirements**

Before a user can use Microsoft's folder redirection, the Windows client must support the feature.

For the latest information about which Windows clients support folder redirection, see the Interoperability Matrix at mysupport.netapp.com/matrix.

**Configuring folder redirection**

You can configure folder redirection using the Windows Properties window. The advantage to using this method is that the Windows user can configure folder redirection without assistance from the SVM administrator.

**Steps**

1. In Windows Explorer, right-click the folder that you want to redirect to a network share.
2. Click **Properties**.
   
   Properties for the share you selected are displayed.
3. In the **Shortcut** tab, click **Target** and specify the path to the network location where you want to redirect the selected folder.
   
   For example, if you want to redirect a folder to the data folder in a home directory that is mapped to Q:\, specify Q:\data as the target.
4. Click **OK**.
   
   For more information about configuring offline folders, consult the Microsoft TechNet Library.

**Related information**

How to access the ~snapshot directory from Windows clients using SMB 2.x

The method that you use to access the ~snapshot directory from Windows clients using SMB 2.x differs from the method used for SMB 1.0. You need to understand how to access the ~snapshot directory when using SMB 2.x connections to successfully access data stored in Snapshot copies.

The SVM administrator controls whether users on Windows clients can view and access the ~snapshot directory on a share by enabling or disabling the showsnapshot share property.

When the showsnapshot share property is disabled, a user on a Windows client using SMB 2.x cannot view the ~snapshot directory and cannot access Snapshot copies within the ~snapshot directory, even when manually entering the path to the ~snapshot directory or to specific Snapshot copies within the directory.

When the showsnapshot share property is enabled, a user on a Windows client using SMB 2.x still cannot view the ~snapshot directory either at the root of the share or within any junction or directory below the root of the share. However, after connecting to a share, the user can access the hidden ~snapshot directory by manually appending \~snapshot to the end of the share path. The hidden ~snapshot directory is accessible from two entry points:

- At the root of the share
- At every junction point in the share space

The hidden ~snapshot directory is not accessible from non-junction subdirectories within the share.

Example

With the configuration shown in the following example, a user on a Windows client with an SMB 2.x connection to the “eng” share can access the ~snapshot directory by manually appending \~snapshot to the share path at the root of the share and at every junction point in the path. The hidden ~snapshot directory is accessible from the following three paths:

- \\vs1\eng\~snapshot
- \\vs1\eng\projects1\~snapshot
- \\vs1\eng\projects2\~snapshot

<table>
<thead>
<tr>
<th>Volume</th>
<th>Junction Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>/</td>
</tr>
<tr>
<td>vs1</td>
<td>/eng</td>
</tr>
<tr>
<td>vs1</td>
<td>/eng/projects1</td>
</tr>
<tr>
<td>vs1</td>
<td>/eng/projects2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Share</th>
<th>Path</th>
<th>Properties</th>
<th>Comment</th>
<th>ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>eng</td>
<td>/eng</td>
<td>oplocks change</td>
<td>Everyone</td>
<td>Full Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>notify browse</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>showsnapshot</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Recovering files and folders using Previous Versions

The ability to use Microsoft Previous Versions is applicable to file systems that support Snapshot copies in some form and have them enabled. Snapshot technology is an integral part of Data ONTAP. Users can recover files and folders from Snapshot copies from their Windows client by using the Microsoft Previous Versions feature.

Previous Versions functionality provides a method for users to browse through the Snapshot copies or to restore data from a Snapshot copy without a storage administrator's intervention. Previous Versions is not configurable. It is always enabled. If the storage administrator has made Snapshot copies available on a share, then the user can use Previous Versions to perform the following tasks:

• Recover files that were accidentally deleted.
• Recover from accidentally overwriting a file.
• Compare versions of file while working.

The data stored in Snapshot copies is read-only. Users must save a copy of a file to another location to make any changes to the file. Snapshot copies are periodically deleted; therefore, users need to create copies of files contained in Previous Versions if they want to indefinitely retain a previous version of a file.

Requirements for using Microsoft Previous Versions

Before you can use Previous Versions with your CIFS server, you need to know which versions of Data ONTAP and SMB, and which Windows clients, support it. You also need to know about the Snapshot copy setting requirement.

Data ONTAP version requirements

Data ONTAP 8.2 and later supports Previous Versions.

SMB protocol version requirements

For Storage Virtual Machine (SVM) with FlexVol volumes, Data ONTAP supports Previous Versions on all versions of SMB.

For SVM with Infinite Volume, Data ONTAP supports Previous Versions on SMB 1.0.

Windows client requirements

Before a user can use Previous Versions to access data in Snapshot copies, the Windows client must support the feature.

For the latest information about which Windows clients support Previous Versions, see the Interoperability Matrix at mysupport.netapp.com/matrix.

Requirements for Snapshot copy settings

To use Previous Versions to access data in Snapshot copies, an enabled Snapshot policy must be associated to the volume containing the data, clients must be able to access to the Snapshot data, and Snapshot copies must exist.
Using the Previous Versions tab to view and manage Snapshot copy data

Users on Windows client machines can use the Previous Versions tab on the Windows Properties window to restore data stored in Snapshot copies without needing to involve the Storage Virtual Machine (SVM) administrator.

About this task

You can only use the Previous Versions tab to view and manage data in Snapshot copies of data stored on the SVM if the administrator has enabled Snapshot copies on the volume containing the share, and if the administrator configures the share to show Snapshot copies.

Steps

1. In Windows Explorer, display the contents of the mapped drive of the data stored on the CIFS server.
2. Right-click the file or folder in the mapped network drive whose Snapshot copies you want to view or manage.
3. Click Properties.
   Properties for the file or folder you selected are displayed.
4. Click the Previous Versions tab.
   A list of available Snapshot copies of the selected file or folder is displayed in the Folder versions: box. The listed Snapshot copies are identified by the Snapshot copy name prefix and the creation timestamp.
5. In the Folder versions: box, right-click the copy of the file or folder that you want to manage.
6. Perform the appropriate action:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Do the following...</th>
</tr>
</thead>
<tbody>
<tr>
<td>View data from that Snapshot copy</td>
<td>Click Open.</td>
</tr>
<tr>
<td>Create a copy of data from that Snapshot copy</td>
<td>Click Copy.</td>
</tr>
</tbody>
</table>

Data in Snapshot copies is read-only. If you want to make modifications to files and folders listed in the Previous Versions tab, you must save a copy of the files and folders that you want to modify to a writable location and make modifications to the copies.

7. After you finish managing Snapshot data, close the Properties dialog box by clicking OK.

For more information about using the Previous Versions tab to view and manage Snapshot data, consult the Microsoft TechNet Library.

Related information


Determining whether Snapshot copies are available for Previous Versions use

You can view Snapshot copies from the Previous Versions tab only if an enabled Snapshot policy is applied to the volume containing the share, and if the volume configuration allows access to Snapshot
copies. Determining Snapshot copy availability is helpful when assisting a user with Previous
Versions access.

Steps
1. Determine whether the volume on which the share data resides has automatic Snapshot copies
   enabled and whether clients have access to Snapshot directories:
   
   ```
   volume show -vserver vserver-name -volume volume-name -fields vserver,volume,snapdir-access,snapshot-policy,snapshot-count
   ```

   The output displays what Snapshot policy is associated with the volume, whether client Snapshot
directory access is enabled, and the number of available Snapshot copies.

2. Determine whether the associated Snapshot policy is enabled:
   
   ```
   volume snapshot policy show -policy policy-name
   ```

3. List the available Snapshot copies:
   
   ```
   volume snapshot show -volume volume_name
   ```

   For more information about configuring and managing Snapshot policies and Snapshot schedules,
see the *Clustered Data ONTAP Data Protection Guide*.

Example
The following example displays information about Snapshot policies associated with the
volume named “data1” that contains the shared data and available Snapshot copies on “data1”.

```
cluster1::> volume show -vserver vs1 -volume data1 -fields vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-------- ------ -------------- --------------- --------------
vs1      data1  true           default         10
```

```
cluster1::> volume snapshot policy show -policy default
Vserver: cluster1
Policy Name Schedules Enabled Comment
------------------ --------- ------- ----------------------------------
default                    3 true    Default policy with hourly, daily & weekly schedules.
Schedule Count Prefix                 SnapMirror Label
---------------- -----     ---------------------- -------------------
hourly               6     hourly                 -
daily                2     daily                  daily
weekly               2     weekly                 weekly
```

```
cluster1::> volume snapshot show -volume data1
---Blocks---
Vserver  Volume  Snapshot                  State        Size Total% Used%
-------- ------- ------------------------- -------- -------- ------ -----
vs1      data1
weekly.2012-12-16_0015    valid       408KB     0%    1%
daily.2012-12-22_0010     valid       420KB     0%    1%
daily.2012-12-23_0010     valid       192KB     0%    0%
weekly.2012-12-23_0015    valid       360KB     0%    1%
hourly.2012-12-23_1405    valid       196KB     0%    0%
hourly.2012-12-23_1505    valid       196KB     0%    0%
hourly.2012-12-23_1605    valid       212KB     0%    0%
hourly.2012-12-23_1705    valid       136KB     0%    0%
hourly.2012-12-23_1805    valid       200KB     0%    0%
hourly.2012-12-23_1905    valid       184KB     0%    0%
```

Related tasks

*Creating a Snapshot configuration to enable Previous Versions access* on page 318
Creating a Snapshot configuration to enable Previous Versions access

The Previous Versions functionality is always available, provided that client access to Snapshot copies is enabled and provided that Snapshot copies exist. If your Snapshot copy configuration does not meet these requirements, you can create a Snapshot copy configuration that does.

Steps

1. If the volume containing the share to which you want to allow Previous Versions access does not have an associated Snapshot policy, associate a Snapshot policy to the volume and enable it by using the `volume modify` command.
   
   For more information about using the `volume modify` command, see the man pages.

2. Enable access to the Snapshot copies by using the `volume modify` command to set the `-snap-dir` option to `true`.
   
   For more information about using the `volume modify` command, see the man pages.

3. Verify that Snapshot policies are enabled and that access to Snapshot directories is enabled by using the `volume show` and `volume snapshot policy show` commands.
   
   For more information about using the `volume show` and `volume snapshot policy show` commands, see the man pages.

   For more information about configuring and managing Snapshot policies and Snapshot schedules, see the *Clustered Data ONTAP Data Protection Guide*

Considerations when restoring directories that contain junctions

There are certain considerations you need to know about when using Previous Versions to restore folders that contain junction points.

When using Previous Versions to restore folders that have child folders that are junction points, the restore can fail with an Access Denied error.

You can determine whether the folder that you are attempting to restore contains a junction by using the `vol show` command with the `-parent` option. You can also use the `vserver security trace` commands to create detailed logs about file and folder access issues.

Related concepts

*Creating and managing data volumes in NAS namespaces* on page 148
Deploying CIFS server-based services

You can deploy a number of CIFS server-based services that can provide you with enhanced functionality for your CIFS deployment. CIFS server-based services include dynamic home directories, SMB access to UNIX symbolic links, BranchCache remote office caching, automatic node referrals, ODX copy offload, and folder security using access-based enumeration (ABE).

Managing home directories

You can use Data ONTAP home directory functionality to create users' home directories on the CIFS server and automatically offer each user a dynamic share to their home directory without creating an individual SMB share for each user.

How clustered Data ONTAP enables dynamic home directories

Clustered Data ONTAP home directories enable you to configure an SMB share that maps to different directories based on the user that connects to it and a set of variables. Instead of having to create separate shares for each user, you can configure a single share with a few home directory parameters to define a user’s relationship between an entry point (the share) and their home directory (a directory on the Storage Virtual Machine (SVM)).

There are four variables that determine how a user is mapped to a directory:

Share name

This is the name of the share that you create that the user connects to. You must set the home directory property for this share.

The share name can use the following dynamic names:

- %w (the user’s Windows user name)
- %d (the user’s Windows domain name)
- %u (the user’s mapped UNIX user name)

To ensure that the share name is unique across all home directories, the share name must contain either the %w or the %u variable. The share name can contain both the %d and the %w variable (for example, %d/%w) or can contain both a static portion and a variable portion to the share name (for example, home_%w).

Share path

This is the relative path, defined by the share and therefore associated with one of the share names, that is appended to each search path to generate the user’s entire home directory path from the root of the SVM. It can be static (for example, home), dynamic (for example, %w), or a combination of the two (for example, eng/%w).

Search paths

This is the set of absolute paths from the root of the SVM that you specify that directs the clustered Data ONTAP search for home directories. You specify one or more search paths by using the vserver cifs home-directory search-path add command. If you specify multiple search paths, clustered Data ONTAP tries them in the order specified until it finds a valid path.

Directory

This is the user’s home directory that you create for the user. It is usually the user’s name. You must create it in one of the directories defined by the search paths.
As an example, consider the following setup:

- User: John Smith
- User domain: acme
- User name: jsmith
- SVM name: vs1
- Home directory share name #1: home_%w - share path: %w
- Home directory share name #2: %w - share path: %d/%w
- Search path #1: /aggr0home/home
- Search path #2: /aggr1home/home
- Search path #3: /aggr2home/home
- Home directory: /aggr1home/home/jsmith

Scenario 1: The user connects to \vs1\home_{jsmith}. This matches the first home directory share name and generates the relative path jsmith. Clustered Data ONTAP now searches for a directory named jsmith by checking each search path in order:

- /aggr0home/home/jsmith does not exist; moving on to search path #2.
- /aggr1home/home/jsmith does exist, therefore search path #3 is not checked; the user is now connected to his home directory.

Scenario 2: The user connects to \vs1\jsmith. This matches the second home directory share name and generates the relative path acme/jsmith. Clustered Data ONTAP now searches for a directory named acme/jsmith by checking each search path in order:

- /aggr0home/home/acme/jsmith does not exist; moving on to search path #2.
- /aggr1home/home/acme/jsmith does not exist; moving on to search path #3.
- /aggr2home/home/acme/jsmith does not exist; the home directory does not exist, therefore the connection fails.

Related tasks

- Adding a home directory share on page 320
- Adding a home directory search path on page 322
- Creating a home directory configuration using the %w and %d variables on page 323
- Configuring home directories using the %u variable on page 325

Adding a home directory share

If you want to use the SMB home directory feature, you must add at least one share with the home directory property included in the share properties.

About this task

You can create a home directory share at the time you create the share by using the vserver cifs share create command, or you can change an existing share into a home directory share at any time by using the vserver cifs share modify command.

To create a home directory share, you must include the homedirectory value in the -share-properties option when you create or modify a share. You can specify the share name and share
path using variables that are dynamically expanded when users connect to their home directories. Available variables that you can use in the path are %w, %d, and %u, corresponding to the Windows user name, domain, and mapped UNIX user name, respectively.

**Steps**

1. Add a home directory share:

   ```
   vserver cifs share create -vserver vs1 -share-name share_name -path path -share-properties homedirectory[,...]
   ```

   - `vserver vserver` specifies the CIFS-enabled Storage Virtual Machine (SVM) on which to add the search path.
   - `share-name share-name` specifies the home directory share name.
   
   In addition to containing one of the required variables, if the share name contains one of the literal strings %w, %u, or %d, you must precede the literal string with a % (percent) character to prevent clustered Data ONTAP from treating the literal string as a variable (for example, %%w).
   
   - The share name must contain either the %w or the %u variable.
   
   - The share name can additionally contain the %d variable (for example, %d/%w) or a static portion in the share name (for example, home1_%w).
   
   - If the share is used by administrators to connect to other users' home directories or to permit users to connect to other users' home directories, the dynamic share name pattern must be preceded by a tilde (~).
   
   The `vserver cifs home-directory modify` is used to enable this access by setting the `-is-home-dirs-access-for-admin-enabled option to true` or by setting the advanced option `-is-home-dirs-access-for-public-enabled to true`.

   - `path path` specifies the relative path to the home directory.

   - `share-properties homedirectory[,...]` specifies the share properties for that share. You must specify the `homedirectory` value. You can specify additional share properties using a comma delimited list.

2. Verify that you successfully added the home directory share by using the `vserver cifs share show` command.

   **Example**

   The following command creates a home directory share named %w. The `oplocks`, `browsable`, and `changenotify` share properties are set in addition to setting the `homedirectory` share property.

   **Note:** This example does not display output for all of the shares on the SVM. Output is truncated.

   ```
   cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w -share-properties oplocks,browsable,changenotify,homedirectory
   vs1::> vserver cifs share show -vserver vs1
   ```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Share</th>
<th>Path</th>
<th>Properties</th>
<th>Comment</th>
<th>ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>%w</td>
<td>%w</td>
<td>oplocks</td>
<td>-</td>
<td>Everyone / Full</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>browsable</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>changenotify</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>homedirectory</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Home directory shares require unique user names

Be careful to assign unique user names when creating home directory shares using the \$w (Windows user name) or \$u (UNIX user name) variables to generate shares dynamically. The share name is mapped to your user name.

Two problems can occur when a static share's name and a user's name are the same:

- When the user lists the shares on a cluster using the `net view` command, two shares with the same user name are displayed.
- When the user connects to that share name, the user is always connected to the static share and cannot access the home directory share with the same name.

For example, there is a share named “administrator” and you have an “administrator” Windows user name. If you create a home directory share and connect to that share, you get connected to the “administrator” static share, not to your “administrator” home directory share.

You can resolve the issue with duplicate share names by following any of these steps:

- Renaming the static share so that it no longer conflicts with the user's home directory share.
- Giving the user a new user name so that it no longer conflicts with the static share name.
- Creating a CIFS home directory share with a static name such as “home” instead of using the \$w parameter to avoid conflicts with the share names.

What happens to static home directory share names after upgrading

Starting with clustered Data ONTAP 8.3, home directory share names must contain either the \$w or the \$u dynamic variable. You should be aware of what happens to existing static home directory share names after upgrading to a version of clustered Data ONTAP with the new requirement.

If your home directory configuration contains static share names and you upgrade to clustered Data ONTAP 8.3 or later, the static home directory share names are not changed and are still valid. However, you cannot create any new home directory shares that do not contain either the \$w or \$u variable.

Requiring that one of these variables is included in the user's home directory share name ensures that every share name is unique across the home directory configuration. If desired, you can change the static home directory share names to names that contain either the \$w or \$u variable.

Adding a home directory search path

If you want to use Data ONTAP SMB home directories, you must add at least one home directory search path.

About this task

You can add a home directory search path by using the `vserver cifs home-directory search-path add` command.
The `vserver cifs home-directory search-path add` command checks the path specified in the `-path` option during command execution. If the specified path does not exist, the command generates a message prompting for whether you want to continue. You choose `y` or `n`. If you choose `y` to continue, Data ONTAP creates the search path. However, you must create the directory structure before you can use the search path in the home directory configuration. If you choose not to continue, the command fails; the search path is not created. You can then create the path directory structure and rerun the `vserver cifs home-directory search-path add` command.

**Steps**

1. Add a home directory search path by entering the following command:

   ```bash
   vserver cifs home-directory search-path add -vserver vserver -path path
   ```

   `-vserver vserver` specifies the CIFS-enabled Storage Virtual Machine (SVM) on which to add the search path.

   `-path path` specifies the directory path to the search path.

2. Verify that you successfully added the search path using the `vserver cifs home-directory search-path show` command.

   **Example**

   The following example adds the path `/home1` to the home directory configuration on SVM vs1.

   ```bash
   cluster::> vserver cifs home-directory search-path add -vserver vs1 -path /home1
   vs1::> vserver cifs home-directory search-path show
   Vserver     Position Path
   ----------- -------- ----------------- 
   vs1         1        /home1
   ```

   The following example attempts to add the path `/home2` to the home directory configuration on SVM vs1. The path does not exist. The choice is made to not continue.

   ```bash
   cluster::> vserver cifs home-directory search-path add -vserver vs1 -path /home2
   Warning: The specified path "/home2" does not exist in the namespace belonging to Vserver "vs1".
   Do you want to continue? {y|n}: n
   ```

**Related concepts**

- How clustered Data ONTAP enables dynamic home directories on page 319

**Related tasks**

- Adding a home directory share on page 320

**Creating a home directory configuration using the `%w` and `%d` variables**

You can create a home directory configuration using the `%w` and `%d` variables. Users can then connect to their home share using dynamically created shares.

**Steps**

1. Optional: Create a qtree to contain user's home directories by entering the following command:
volume qtree create -vserver vserver_name -qtree-path qtree_path

2. Optional: Verify that the qtree is using the correct security style by entering the following command:

   volume qtree show

3. Optional: If the qtree is not using the desired security style, change the security style using the volume qtree security command.

4. Add a home directory share by entering the following command:

   vserver cifs share create -vserver vserver -share-name %w -path %d/%w -share-properties homedirectory[,....]

   -vserver vserver specifies the CIFS-enabled Storage Virtual Machine (SVM) on which to add the search path.

   -share-name %w specifies the home directory share name. Data ONTAP dynamically creates the share name as each user connects to their home directory. The share name will be of the form windows_user_name.

   -path %d/%w specifies the relative path to the home directory. The relative path is dynamically created as each user connects to their home directory and will be of the form domain/ windows_user_name.

   -share-properties homedirectory[,....] specifies the share properties for that share. You must specify the homedirectory value. You can specify additional share properties using a comma delimited list.

5. Verify that the share has the desired configuration using the vserver cifs share show command.

6. Add a home directory search path by entering the following command:

   vserver cifs home-directory search-path add -vserver vserver -path path

   -vserver vserver specifies the CIFS-enabled SVM on which to add the search path.

   -path path specifies the absolute directory path to the search path.

7. Verify that you successfully added the search path using the vserver cifs home-directory search-path show command.

8. For users with a home directory, create a corresponding directory in the qtree or volume designated to contain home directories.

   For example, if you created a qtree with the path of /vol/voll/users and the user name whose directory you want to create is mydomain\user1, you would create a directory with the following path: /vol/voll/users/mydomain/user1.

   If you created a volume named “home1” mounted at /home1, you would create a directory with the following path: /home1/mydomain/user1.

9. Verify that a user can successfully connect to the home share either by mapping a drive or connecting using the UNC path.

   For example, if user mydomain\user1 wants to connect to the directory created in Step 8 that is located on SVM vs1, user1 would connect using the UNC path \\vs1\user1.

Example

The commands in the following example create a home directory configuration with the following settings:
• The share name is %w.
• The relative home directory path is %d/%w.
• The search path that is used to contain the home directories, /home1, is a volume configured with NTFS security style.
• The configuration is created on SVM vs1.

You can use this type of home directory configuration when users access their home directories from Windows hosts. You can also use this type of configuration when users access their home directories from Windows and UNIX hosts and the file system administrator uses Windows-based users and groups to control access to the file system.

```
class::> vserver cifs share create -vserver vs1 -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory
```
```
class::> vserver cifs share show -vserver vs1 -share-name %w
```
```
Vserver: vs1
Share: %w
CIFS Server NetBIOS Name: VS1
Path: %d/%w
Share Properties: oplocks
         browsable
   changenotify
   homedirectory
Symlink Properties: enable
  File Mode Creation Mask: -
Directory Mode Creation Mask: -
     Share Comment: -
                   Share ACL: Everyone / Full Control
  File Attribute Cache Lifetime: -
     Volume Name: -
Offline Files: manual
  Vscan File-Operations Profile: standard
```
```
class::> vserver cifs home-directory search-path add -vserver vs1 -path /home1
```
```
class::> vserver cifs home-directory search-path show
Vserver    Position Path
----------- -------- -----------------
vs1         1        /home1
```

Related concepts

Additional home directory configurations on page 328

Related tasks

Configuring home directories using the %u variable on page 325
Displaying information about an SMB user's home directory path on page 329

Configuring home directories using the %u variable

You can create a home directory configuration where you designate the share name using the %w variable but you use the %u variable to designate the relative path to the home directory share. Users can then connect to their home share using dynamically shares created using their Windows user name without being aware of the actual name or path of the home directory.

Steps

1. Optional: Create a qtree to contain user's home directories by entering the following command:
   
   ```
   volume qtree create -vserver vserver_name -qtrees-path qtree_path
   ```
2. Optional: Verify that the qtree is using the correct security style by entering the following command:

```
volume qtree show
```

3. Optional: If the qtree is not using the desired security style, change the security style using the `volume qtree security` command.

4. Add a home directory share by entering the following command:

```
vserver cifs share create -vserver vserver -share-name $w -path $u -share-properties homedirectory ,...
```

- `vserver vserver` specifies the CIFS-enabled Storage Virtual Machine (SVM) on which to add the search path.
- `-share-name $w` specifies the home directory share name. The share name is dynamically created as each user connects to their home directory and is of the form `windows_user_name`.
  
  **Note:** You can also use the `$u` variable for the `-share-name` option. This creates a relative share path that uses the mapped UNIX user name.

- `-path $u` specifies the relative path to the home directory. The relative path is created dynamically as each user connects to their home directory and is of the form `mapped_UNIX_user_name`.
  
  **Note:** The value for this option can contain static elements as well. For example, `eng/%u`.

- `-share-properties homedirectory[,]` specifies the share properties for that share. You must specify the `homedirectory` value. You can specify additional share properties using a comma delimited list.

5. Verify that the share has the desired configuration using the `vserver cifs share show` command.

6. Add a home directory search path by entering the following command:

```
vserver cifs home-directory search-path add -vserver vserver -path path
```

- `vserver vserver` specifies the CIFS-enabled SVM on which to add the search path.
- `-path path` specifies the absolute directory path to the search path.

7. Verify that you successfully added the search path using the `vserver cifs home-directory search-path show` command.

8. Optional: If the UNIX user does not exist, create the UNIX user using the `vserver services unix-user create` command.

   **Note:** The UNIX user name to which you map the Windows user name must exist before mapping the user.

9. Optional: Create a name mapping for the Windows user to the UNIX user using the following command:

```
vserver name-mapping create -vserver vserver_name -direction win-unix -priority integer -pattern windows_user_name -replacement unix_user_name
```

   **Note:** If name mappings already exist that map Windows users to UNIX users, you do not have to perform the mapping step.

The Windows user name is mapped to the corresponding UNIX user name. When the Windows user connects to their home directory share, they connect to a dynamically created home directory with a share name that corresponds to their Windows user name without being aware that the directory name corresponds to the UNIX user name.
10. For users with a home directory, create a corresponding directory in the qtree or volume designated to contain home directories.

For example, if you created a qtree with the path of /vol/vol1/users and the mapped UNIX user name of the user whose directory you want to create is “unixuser1”, you would create a directory with the following path: /vol/vol1/users/unixuser1.

If you created a volume named “home1” mounted at /home1, you would create a directory with the following path: /home1/unixuser1.

11. Verify that a user can successfully connect to the home share either by mapping a drive or connecting using the UNC path.

For example, if user mydomain\user1 maps to UNIX user unixuser1 and wants to connect to the directory created in Step 10 that is located on SVM vs1, user1 would connect using the UNC path \vs1\user1.

### Example

The commands in the following example create a home directory configuration with the following settings:

- The share name is %w.
- The relative home directory path is %u.
- The search path that is used to contain the home directories, /home1, is a volume configured with UNIX security style.
- The configuration is created on SVM vs1.

You can use this type of home directory configuration when users access their home directories from both Windows hosts or Windows and UNIX hosts and the file system administrator uses UNIX-based users and groups to control access to the file system.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path %u
   -share-properties oplocks,browsable,changenotify,homedirectory
cluster::> vserver cifs share show -vserver vs1 -share-name %u

Vserver: vs1
Share: %w
CIFS Server NetBIOS Name: VS1
Path: %u
Share Properties: oplocks
browsable
changenotify
homedirectory

Symlink Properties: enable
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path /home1
cluster::> vserver cifs home-directory search-path show -vserver vs1

Vserver  Position  Path
---------  ------  -----------------
vs1        1       /home1

cluster::> vserver name-mapping create -vserver vs1 -direction win-unix
   -position 5 -pattern user1 -replacement unixuser1
cluster::> vserver name-mapping show -pattern user1
```
Related concepts

*Additional home directory configurations* on page 328

Related tasks

*Creating a home directory configuration using the %w and %d variables* on page 323
*Displaying information about an SMB user's home directory path* on page 329

Additional home directory configurations

You can create additional home directory configurations using the `%w`, `%d`, and `%u` variables, which enables you to customize the home directory configuration to meet your needs.

You can create a number of home directory configurations using a combination of variables and static strings in the share names and search paths. The following table provides some examples illustrating how to create different home directory configurations:

<table>
<thead>
<tr>
<th>Paths created when /vol1/user contains home directories...</th>
<th>Share command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>To create a share path <code>\\vs1\~win_username</code> that directs the user to <code>/vol1/user/</code> <code>win_username</code></td>
<td><code>vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,home directory</code></td>
</tr>
<tr>
<td>To create a share path <code>\\vs1\win_username</code> that directs the user to <code>/vol1/user/domain/</code> <code>win_username</code></td>
<td><code>vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,home directory</code></td>
</tr>
<tr>
<td>To create a share path <code>\\vs1\win_username</code> that directs the user to <code>/vol1/user/</code> <code>unix_username</code></td>
<td><code>vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,home directory</code></td>
</tr>
<tr>
<td>To create a share path <code>\\vs1\unix_username</code> that directs the user to <code>/vol1/user/</code> <code>unix_username</code></td>
<td><code>vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,home directory</code></td>
</tr>
</tbody>
</table>

Commands for managing search paths

There are specific Data ONTAP commands for managing search paths for CIFS home directory configurations. For example, there are commands for adding, removing, and displaying information about search paths. There is also a command for changing the search path order.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a search path</td>
<td><code>vserver cifs home-directory search-path add</code></td>
</tr>
<tr>
<td>Display search paths</td>
<td><code>vserver cifs home-directory search-path show</code></td>
</tr>
</tbody>
</table>
If you want to... | Use this command...
-----------------|----------------------------------
Change the search path order | vserver cifs home-directory search-path reorder
Remove a search path | vserver cifs home-directory search-path remove

See the man page for each command for more information.

**Displaying information about an SMB user’s home directory path**

You can display an SMB user's home directory path on the Storage Virtual Machine (SVM), which can be used if you have multiple CIFS home directory paths configured and you want to see which path holds the user's home directory.

**Step**

1. Display the home directory path by using the `vserver cifs home-directory show-user` command.

   **Example**
   
   ```
   vserver cifs home-directory show-user -vserver vs1 -username user1
   ```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>User</th>
<th>Home Dir Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>user1</td>
<td>/home/user1</td>
</tr>
</tbody>
</table>

**Related tasks**

*Managing accessibility to users’ home directories* on page 329

**Managing accessibility to users’ home directories**

By default, a user’s home directory can be accessed only by that user and by Windows administrators. For shares where the dynamic name of the share is preceded with a tilde (~), you can enable or disable access to users’ home directories by Windows administrators or by any other user (public access).

**Before you begin**

Home directory shares on the Storage Virtual Machine (SVM) must be configured with dynamic share names that are preceded with a tilde (~). The following cases illustrate share naming requirements:

<table>
<thead>
<tr>
<th>Home directory share name</th>
<th>Example of command to connect to the share</th>
</tr>
</thead>
<tbody>
<tr>
<td><del>%d</del>%w</td>
<td>net use * //IPaddress/<del>domain</del>user /u:credentials</td>
</tr>
<tr>
<td>~%w</td>
<td>net use * //IPaddress/~user /u:credentials</td>
</tr>
<tr>
<td>abc~%w</td>
<td>net use * //IPaddress/abc~user /u:credentials</td>
</tr>
</tbody>
</table>
Step

1. Perform the appropriate action:

<table>
<thead>
<tr>
<th>If you want to enable or disable access to users' home directories to...</th>
<th>Enter the following...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows administrators</td>
<td>vserver cifs home-directory modify -vserver vserver_name -is-home-dirs-access-for-admin-enabled {true</td>
</tr>
<tr>
<td></td>
<td>The default is true.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Any user (public access)</th>
<th>a. Set the privilege level to advanced:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>set -privilege advanced</code></td>
</tr>
<tr>
<td>b. Enable or disable access:</td>
<td>vserver cifs home-directory modify -vserver vserver_name -is-home-dirs-access-for-public-enabled {true</td>
</tr>
<tr>
<td></td>
<td>The default is false.</td>
</tr>
<tr>
<td>c. Return to the admin privilege level:</td>
<td><code>set -privilege admin</code></td>
</tr>
</tbody>
</table>

Example

The following example enables access to users’ home directories to Windows administrators:

```
vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-admin-enabled false
```

Example

The following example enables public access to users' home directories:

```
set -privilege advanced
vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-public-enabled true
set -privilege admin
```

Related tasks

Displaying information about an SMB user's home directory path on page 329

Configuring SMB client access to UNIX symbolic links

You can configure the CIFS server to provide SMB client access to UNIX symbolic links. The symbolic links can point to files within the volume that contain the share, or to files that are contained in other volumes on the Storage Virtual Machine (SVM), or even to volumes contained on other SVMs.
How Data ONTAP enables you to provide SMB client access to UNIX symbolic links

You must understand certain concepts about how Data ONTAP enables you to manage symbolic links. This is important to provide access to SMB users connecting to the Storage Virtual Machine (SVM).

A symbolic link is a file created in a UNIX environment that contains a reference to another file or directory. If a client accesses a symbolic link, it is redirected to the target file or directory that the symbolic link refers to.

Data ONTAP provides SMB clients the ability to follow UNIX symbolic links configured on the SVM. This feature is optional and you can configure it on a per-share basis with one of the following settings:

- Enabled with read/write access
- Enabled with read-only access
- Disabled by hiding symbolic links from SMB clients
- Disabled with no access to symbolic links from SMB clients

There are two types of symbolic links:

Relative
A relative symbolic link contains a reference to the file or directory relative to its parent directory. Therefore, the path of the file it is referring to should not begin with a slash (/).

If you enable symbolic links on a share, relative symbolic links work without further configuration.

Absolute
An absolute symbolic link contains a reference to a file or directory in the form of an absolute path. Therefore, the path of the file it is referring to should begin with a slash (/).

It is treated as an absolute path location of the file from the root of the file system. An absolute symbolic link can refer to a file or directory within or outside of the file system of the symbolic link. If the target is not in the same local file system, the symbolic link is called a widelink. If you enable symbolic links on a share, absolute symbolic links do not work right away. You must first create a mapping between the UNIX path of the symbolic link to the destination CIFS path. When creating absolute symbolic link mappings, you specify whether it is a local or widelink. If you create an absolute symbolic link to a file or directory outside of the local share but set the locality to local, Data ONTAP disallows access to the target.

Note that if a client attempts to delete a local symbolic link (absolute or relative), only the symbolic link is deleted, not the target file or directory. However, if a client attempts to delete a widelink, it might delete the actual target file or directory that the widelink refers to. Data ONTAP does not have control over this because the client can explicitly open the target file or directory outside the SVM and delete it.

Related concepts

*Information you need when creating SMB shares* on page 176
Limits when configuring UNIX symbolic links for SMB access

You need to be aware of certain limits when configuring UNIX symbolic links for SMB access.

<table>
<thead>
<tr>
<th>Limit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>45</td>
<td>Maximum length of the CIFS server name that you can specify when using an FQDN for the CIFS server name. <strong>Note:</strong> You can alternatively specify the CIFS server name as a NetBIOS name, which is limited to 15 characters.</td>
</tr>
<tr>
<td>80</td>
<td>Maximum length of the share name.</td>
</tr>
<tr>
<td>256</td>
<td>Maximum length of the UNIX path that you can specify when creating a symbolic link or when modifying an existing symbolic link's UNIX path. The UNIX path must start with a “/” (slash) and end with a “/”. Both the beginning and ending slashes count as part of the 256-character limit.</td>
</tr>
<tr>
<td>256</td>
<td>Maximum length of the CIFS path that you can specify when creating a symbolic link or when modifying an existing symbolic link's CIFS path. The CIFS path must start with a “/” (slash) and end with a “/”. Both the beginning and ending slashes count as part of the 256-character limit.</td>
</tr>
</tbody>
</table>

Related tasks

*Creating symbolic link mappings for SMB shares* on page 335

How to control automatic DFS advertisements in clustered Data ONTAP with a CIFS server option

A CIFS server option has been added that controls how DFS capabilities are advertised to SMB clients when connecting to shares. Because clustered Data ONTAP uses DFS referrals when clients access symbolic links over SMB, you should be aware of what the impact is when disabling or enabling this option.

In clustered Data ONTAP 8.2 through 8.2.2, the CIFS servers on Storage Virtual Machines (SVMs) always advertise to SMB clients that they are DFS capable. However, even though the CIFS servers always advertise that they are DFS capable, symbolic link access for SMB is managed on a share-by-share basis by setting a share parameter. By using the share parameter, you can set symbolic link access for SMB to one of three access levels:

- Enabled for read and write access
- Enabled for read-only access
- Disabled, either by setting the value of this parameter to hide symlinks or by setting the parameter to null (“”)

Starting with Data ONTAP 8.2.3 in the 8.2 release family and with Data ONTAP 8.3 and later, a CIFS server option determines whether the CIFS servers automatically advertise that they are DFS capable to SMB clients. By default, this option is enabled and the CIFS server always advertises that it is DFS capable to SMB clients (even when connecting to shares where access to symbolic links is disabled). If you want the CIFS server to advertise that it is DFS capable to clients only when they are connecting to shares where access to symbolic links is enabled, you can disable this option.

You should be aware of what happens when this option is disabled:

- The share configurations for symbolic links is unchanged.
• If the share parameter is set to allow symbolic link access (either read-write access or read-only access), the CIFS server advertises DFS capabilities to clients connecting to that share. Client connections and access to symbolic links continue without interruption.

• If the share parameter is set to not allow symbolic link access (either by disabling access or if the value for the share parameter is null), the CIFS server does not advertise DFS capabilities to clients connecting to that share.

Because clients have cached information that the CIFS server is DFS capable and it is no longer advertising that it is, clients that are connected to shares where symbolic link access is disabled might not be able to access these shares after the CIFS server option is disabled. After the option is disabled, you might need to reboot clients that are connected to these shares, thus clearing the cached information.

These changes do not apply to SMB 1.0 connections.

Managing whether the CIFS server automatically advertises DFS capabilities

You can set a CIFS server option to determine whether CIFS servers automatically advertise DFS capabilities to SMB 2.x and SMB 3.0 clients connecting to shares. You can disable automatic advertisements in cases where you have applications that will not make connections to shares that advertise DFS capabilities.

About this task

Clustered Data ONTAP uses DFS referrals in the implementation of symbolic links for SMB access. You should keep the following in mind when deciding whether to enable or disable this option:

• If automatic DFS advertisements are enabled, the CIFS server always advertises DFS capabilities to SMB 2.x and SMB 3.0 clients connecting to a share regardless of whether symbolic link access for CIFS is enabled on that share.

This is the default setting.

• If automatic DFS advertisements are disabled, the CIFS server advertises DFS capabilities to SMB 2.x and SMB 3.0 clients only when the clients are connecting to shares where symbolic link access is enabled (either read-write or read-only access) and does not advertise DFS capabilities to clients if they are connecting to shares where symbolic link access is disabled.

Clients that are connected to shares where symbolic link access is disabled might not be able to access these shares after the CIFS server option is disabled. This is because the clients have cached information that the CIFS server is DFS capable, and it is no longer advertising that it is. This causes reconnections to SMB shares to fail. There are two ways to manage this:

• Before disabling the option, you can change the share setting on all shares to allow either read-write or read-only access.

• If it is not possible to change the settings for shares where symbolic link access is disabled, after the option is disabled, you can reboot any affected clients that are connected to these shares, thus clearing the cached information.

Steps

1. Set the privilege level to advanced:
   
   set -privilege advanced

2. Configure the DFS referral option setting:
   
   vserver cifs options modify -vserver vserver_name -is-advertise-dfs-enabled {true|false}

Deploying CIFS server-based services | 333
3. Verify that the option is set to the desired value:

```
vserver cifs options show -vserver vserver_name
```

4. Return to the admin privilege level:

```
set -privilege admin
```

**Configuring UNIX symbolic link support on SMB shares**

You can configure UNIX symbolic link support on SMB shares by specifying a symbolic link share-property setting when you create SMB shares or at any time by modifying existing SMB shares. UNIX symbolic link support is enabled by default. You can also disable UNIX symbolic link support on a share.

**About this task**

When configuring UNIX symbolic link support for SMB shares, you can choose one of the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>This setting specifies that symbolic links are enabled for read-write access. This is the default setting.</td>
</tr>
<tr>
<td>read_only</td>
<td>This setting specifies that symbolic links are enabled for read-only access. This setting does not apply to widelinks. Widelink access is always read-write.</td>
</tr>
<tr>
<td>hide</td>
<td>This setting specifies that SMB clients are prevented from seeing symbolic links.</td>
</tr>
<tr>
<td>&quot;&quot; (null, not set)</td>
<td>This setting disables symbolic links on the share.</td>
</tr>
<tr>
<td>- (not set)</td>
<td>This setting disables symbolic links on the share.</td>
</tr>
</tbody>
</table>

**Steps**

1. Configure or disable symbolic link support:

<table>
<thead>
<tr>
<th>If it is...</th>
<th>Enter...</th>
</tr>
</thead>
<tbody>
<tr>
<td>A new SMB share</td>
<td>vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink-properties {enable</td>
</tr>
<tr>
<td>An existing SMB share</td>
<td>vserver cifs share modify -vserver vserver_name -share-name share_name -symlink-properties {enable</td>
</tr>
</tbody>
</table>

2. Verify that the SMB share configuration is correct:

```
vserver cifs share show -vserver vserver_name -share-name share_name -instance
```

**Example**

The following command creates an SMB share named “data1” with the UNIX symbolic link configuration set to `enable`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name datal -path / datal -symlink-properties enable
cluster1::> vserver cifs share show -vserver vs1 -share-name datal -instance
Vserver: vs1
```
Creating symbolic link mappings for SMB shares

You can create mappings of UNIX symbolic links for SMB shares. You can either create a relative symbolic link, which refers to the file or folder relative to its parent folder, or you can create an absolute symbolic link, which refers to the file or folder using an absolute path.

About this task

Widelinks are not accessible from Mac OS X clients if you use SMB 2.x. When a user attempts to connect to a share using widelinks from a Mac OS X client, the attempt fails. However, you can use widelinks with Mac OS X clients if you use SMB 1.

Step

1. To create symbolic link mappings for SMB shares, enter the following command:

```bash
vserver cifs symlink create -vserver virtual_server_name -unix-path path -share-name share_name -cifs-path path [-cifs-server server_name] [-locality {local|widelink}] [-home-directory {true|false}]
```

- `vserver virtual_server_name` specifies the Storage Virtual Machine (SVM) name.
- `-unix-path path` specifies the UNIX path. The UNIX path must begin with a slash (/) and must end with a slash (/).
- `-share-name share_name` specifies the name of the SMB share to map.
- `-cifs-path path` specifies the CIFS path. The CIFS path must begin with a slash (/) and must end with a slash (/).
- `-cifs-server server_name` specifies the CIFS server name. The CIFS server name can be specified as a DNS name (for example, mynetwork.cifs.server.com), IP address, or NetBIOS name. The NetBIOS name can be determined by using the `vserver cifs show` command. If this optional parameter is not specified, the default value is the NetBIOS name of the local CIFS server.
- `-locality {local|widelink}` specifies whether to create a local or wide symbolic link. A local symbolic link maps to the local SMB share, and a wide symbolic link maps to any SMB share on the network. If you do not specify this optional parameter, the default value is `widelink`.

Related tasks

- [Creating an SMB share on a CIFS server](#) on page 177
- [Creating symbolic link mappings for SMB shares](#) on page 335
-home-directory \{true|false\} specifies whether the target share is a home directory. Even though this parameter is optional, you must set this parameter to true when the target share is configured as a home directory. The default is false.

**Example**

The following command creates a symbolic link mapping on the SVM named vs1. It has the UNIX path /src/, the SMB share name “SOURCE”, the CIFS path /mycompany/source/, and the CIFS server IP address 123.123.123.123, and it is a widelink.

```
classeter1::> vserver cifs symlink create -vserver vs1 -unix-path /src/ -share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server 123.123.123.123 -locality widelink
```

**Related concepts**

*How Data ONTAP enables you to provide SMB client access to UNIX symbolic links* on page 331

**Related tasks**

*Configuring UNIX symbolic link support on SMB shares* on page 334

**Commands for managing symbolic link mappings**

There are specific Data ONTAP commands for managing symbolic link mappings.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a symbolic link mapping</td>
<td>vserver cifs symlink create</td>
</tr>
<tr>
<td>Display information about symbolic link mappings</td>
<td>vserver cifs symlink show</td>
</tr>
<tr>
<td>Modify a symbolic link mapping</td>
<td>vserver cifs symlink modify</td>
</tr>
<tr>
<td>Delete a symbolic link mapping</td>
<td>vserver cifs symlink delete</td>
</tr>
</tbody>
</table>

See the man page for each command for more information.

**Using BranchCache to cache SMB share content at a branch office**

BranchCache was developed by Microsoft to enable caching of content on computers local to requesting clients. The Data ONTAP implementation of BranchCache can reduce wide-area network (WAN) utilization and provide improved access response time when users in a branch office access content stored on Storage Virtual Machines (SVMs) using SMB.

If you configure BranchCache, Windows BranchCache clients first retrieve content from the SVM and then cache the content on a computer within the branch office. If another BranchCache-enabled client in the branch office requests the same content, the SVM first authenticates and authorizes the requesting user. The SVM then determines whether the cached content is still up-to-date and, if it is, sends the client metadata about the cached content. The client then uses the metadata to retrieve content directly from the locally based cache.

**Related concepts**

*Using offline files to allow caching of files for offline use* on page 307
Requirements, considerations, and recommendations

Before you can use the BranchCache feature with your Storage Virtual Machine (SVM) with FlexVol volumes, you need to be aware of certain requirements, considerations, and recommendations. For example, you need to know about Data ONTAP support for the feature. You also need to know about SMB version support and about supported Windows hosts.

Related tasks

Configuring BranchCache on the CIFS server on page 340

BranchCache version support

You should be aware of which BranchCache versions Data ONTAP supports.

Data ONTAP supports BranchCache 1 and the enhanced BranchCache 2:

- When you configure BranchCache on the CIFS server for the Storage Virtual Machine (SVM), you can enable BranchCache 1, BranchCache 2, or all versions.
  By default, all versions are enabled.

- If you enable only BranchCache 2, the remote office Windows client machines must support BranchCache 2.
  Only SMB 3.0 or later clients support BranchCache 2.

For more information about BranchCache versions, see the Microsoft TechNet Library.

Related information


Network protocol support requirements

You must be aware of the network protocol requirements for implementing Data ONTAP BranchCache.

You can implement the Data ONTAP BranchCache feature over IPv4 and IPv6 networks using SMB 2.1 or later.

All CIFS servers and branch office machines participating in the BranchCache implementation must have the SMB 2.1 or later protocol enabled. SMB 2.1 has protocol extensions that allow a client to participate in a BranchCache environment. This is the minimum SMB protocol version that offers BranchCache support. SMB 2.1 supports version BranchCache version 1.

If you want to use BranchCache version 2, SMB 3.0 is the minimum supported version. All CIFS servers and branch office machines participating in a BranchCache 2 implementation must have SMB 3.0 or later enabled.

If you have remote offices where some of the clients support only SMB 2.1 and some of the clients support SMB 3.0, you can implement a BranchCache configuration on the CIFS server that provides caching support over both BranchCache 1 and BranchCache 2.

Note: Even though the Microsoft BranchCache feature supports using both the HTTP/HTTPS and SMB protocols as file access protocols, Data ONTAP BranchCache only supports the use of SMB.

Data ONTAP and Windows hosts version requirements

Data ONTAP and branch office Windows hosts must meet certain version requirements before you can configure BranchCache.

Before configuring BranchCache, you must ensure that the version of Data ONTAP on the cluster and participating branch office clients support SMB 2.1 or later and support the BranchCache feature.
If you configure Hosted Cache mode, you must also ensure that you use a supported host for the cache server.

BranchCache 1 is supported on the following Data ONTAP versions and Windows hosts:

- Content server: Storage Virtual Machine (SVM) with Data ONTAP 8.2 or later
- Cache server: Windows Server 2008 R2 or Windows Server 2012 or later
- Peer or client: Windows 7 Enterprise, Windows 7 Ultimate, Windows 8, Windows Server 2008 R2 or Windows Server 2012 or later

BranchCache 2 is supported on the following Data ONTAP versions and Windows hosts:

- Content server: SVM with Data ONTAP 8.2 or later
- Cache server: Windows Server 2012 or later
- Peer or client: Windows 8 or Windows Server 2012 or later

For the latest information about which Windows clients support BranchCache, see the Interoperability Matrix at mysupport.netapp.com/matrix.

Reasons Data ONTAP invalidates BranchCache hashes

Understanding the reasons why Data ONTAP invalidates hashes can be helpful as you plan your BranchCache configuration. It can help you decide which operating mode you should configure and can help you choose on which shares to enable BranchCache.

Data ONTAP must manage BranchCache hashes to ensure that hashes are valid. If a hash is not valid, Data ONTAP invalidates the hash and computes a new hash the next time that content is requested, assuming that BranchCache is still enabled.

Data ONTAP invalidates hashes for the following reasons:

- The server key is modified.
  If the server key is modified, Data ONTAP invalidates all hashes in the hash store.

- A hash is flushed from the cache because the BranchCache hash store maximum size has been reached.
  This is a tunable parameter and can be modified to meet your business requirements.

- A file is modified either through SMB or NFS access.

- A file for which there are computed hashes is restored using the `snap restore` command.

- A volume that contains SMB shares that are BranchCache-enabled is restored using the `snap restore` command.

Considerations when choosing the hash store location

When configuring BranchCache, you choose where to store hashes and what size the hash store should be. Understanding certain considerations when choosing the hash store location and size can help you plan your BranchCache configuration on a CIFS-enabled Storage Virtual Machine (SVM).

- You should locate the hash store on a volume where atime updates are permitted.
  The access time on a hash file is used to keep frequently accessed files in the hash store. If atime updates are disabled, the creation time is used for this purpose. It is preferable to use atime to track frequently used files.

- You cannot store hashes on read-only file systems such as SnapMirror destinations and SnapLock volumes.
• If the maximum size of the hash store is reached, older hashes are flushed to make room for new hashes.
   You can increase the maximum size of the hash store to reduce the amount of hashes that are flushed from the cache.

• If the volume on which you store hashes is unavailable or full, or if there is an issue with intra-cluster communication where the BranchCache service cannot retrieve hash information, BranchCache services are not available.
   The volume might be unavailable because it is offline or because the storage administrator specified a new location for the hash store.
   This does not cause issues with file access. If access to the hash store is impeded, Data ONTAP returns a Microsoft-defined error to the client, which causes the client to request the file using the normal SMB read request.

Related concepts
   *Managing and monitoring the BranchCache configuration* on page 346

Related tasks
   *Configuring BranchCache on the CIFS server* on page 340

BranchCache recommendations

Before you configure BranchCache, there are certain recommendations you should keep in mind when deciding on which SMB shares you want to enable BranchCache caching.

You should keep the following recommendations in mind when deciding on which operating mode to use and on which SMB shares to enable BranchCache:

• The benefits of BranchCache are reduced when the data to be remotely cached changes frequently.
• BranchCache services are beneficial for shares containing file content that is reused by multiple remote office clients or by file content that is repeatedly accessed by a single remote user.
• Consider enabling caching for read-only content such as data in Snapshot copies and SnapMirror destinations.

Configuring BranchCache

You configure BranchCache on your CIFS server using Data ONTAP commands. To implement BranchCache, you must also configure your clients, and optionally your hosted cache servers at the branch offices where you want to cache content.

If you configure BranchCache to enable caching on a share-by-share basis, you must enable BranchCache on the SMB shares for which you want to provide BranchCache caching services.

Prerequisites for configuring BranchCache

After meeting some prerequisites, you can set up BranchCache.

The following requirements must be met before configuring BranchCache on the CIFS server for your Storage Virtual Machine (SVM):

• Data ONTAP 8.2 or later must be installed on all nodes in the cluster.
• CIFS must be licensed and a CIFS server must be configured.
• IPv4 or IPv6 network connectivity must be configured.
• For BranchCache 1, SMB 2.1 or later must be enabled.
For BranchCache 2, SMB 3.0 must be enabled and the remote Windows clients must support BranchCache 2.

### Configuring BranchCache on the CIFS server

You can configure BranchCache to provide BranchCache services on a per-share basis. Alternatively, you can configure BranchCache to automatically enable caching on all SMB shares.

#### About this task

You can configure BranchCache on SVMs with FlexVol volumes.

- You can create an all-shares BranchCache configuration if you want to offer caching services for all content contained within all SMB shares on the CIFS server.
- You can create a per-share BranchCache configuration if you want to offer caching services for content contained within selected SMB shares on the CIFS server.

You must specify the following parameters when configuring BranchCache:

<table>
<thead>
<tr>
<th>Required parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SVM name</strong></td>
<td>BranchCache is configured on a per SVM basis. You must specify on which CIFS-enabled SVM you want to configure the BranchCache service.</td>
</tr>
<tr>
<td><strong>Path to hash store</strong></td>
<td>BranchCache hashes are stored in regular files on the SVM volume. You must specify the path to an existing directory where you want Data ONTAP to store the hash data. The BranchCache hash path must be read-writable. Read-only paths, such as Snapshot directories are not allowed. You can store hash data in a volume that contains other data or you can create a separate volume to store hash data. If the SVM is an SVM disaster recovery source, the hash path cannot be on the root volume. This is because the root volume is not replicated to the disaster recovery destination. The hash path can contain blanks and any valid file name characters.</td>
</tr>
</tbody>
</table>

You can optionally specify the following parameters:

<table>
<thead>
<tr>
<th>Optional parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Supported Versions</strong></td>
<td>Data ONTAP support BranchCache 1 and 2. You can enable version 1, version 2, or both versions. The default is to enable both versions.</td>
</tr>
<tr>
<td><strong>Maximum size of hash store</strong></td>
<td>You can specify the size to use for the hash data store. If the hash data exceeds this value, Data ONTAP deletes older hashes to make room for newer hashes. The default size for the hash store is 1 GB. BranchCache performs more efficiently if hashes are not discarded in an overly aggressive manner. If you determine that hashes are discarded frequently because the hash store is full, you can increase the hash store size by modifying the BranchCache configuration.</td>
</tr>
</tbody>
</table>
### Optional parameters

| **Server key** | You can specify a server key that the BranchCache service uses to prevent clients from impersonating the BranchCache server. If you do not specify a server key, one is randomly generated when you create the BranchCache configuration. You can set the server key to a specific value so that if multiple servers are providing BranchCache data for the same files, clients can use hashes from any server using that same server key. If the server key contains any spaces, you must enclose the server key in quotation marks. |
| **Operating mode** | The default is to enable BranchCache on a per-share basis. |
| **Description** |  |

#### Operating mode

- **To create a BranchCache configuration where you enable BranchCache on a per-share basis, you can either not specify this optional parameter or you can specify `per-share`.**
- **To automatically enable BranchCache on all shares, you must set the operating mode to `all-shares`.**

### Steps

1. Enable SMB 2.1 and 3.0 as needed:
   a. Set the privilege level to advanced:
      ```bash
      set -privilege advanced
      ```
   b. Check the configured SVM SMB settings to determine whether all needed versions of SMB are enabled:
      ```bash
      vserver cifs options show -vserver vserver_name
      ```
   c. If necessary, enable SMB 2.1:
      ```bash
      vserver cifs options modify -vserver vserver_name -smb2-enabled true
      ```
      The command enables both SMB 2.0 and SMB 2.1.
   d. If necessary, enable SMB 3.0:
      ```bash
      vserver cifs options modify -vserver vserver_name -smb3-enabled true
      ```
   e. Return to the admin privilege level:
      ```bash
      set -privilege admin
      ```
2. Configure BranchCache:
   ```bash
   vserver cifs branchcache create -vserver vserver_name -hash-store-path path [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-enable|v2-enable|enable-all} [-server-key text] -operating-mode {per-share|all-shares}]
   ```
   The specified hash storage path must exist and must reside on a volume managed by the SVM. The path must also be located on a read-writable volume. The command fails if the path is read-only or does not exist.
   If you want to use the same server key for additional SVM BranchCache configurations, record the value you enter for the server key. The server key does not appear when you display information about the BranchCache configuration.
3. Verify that the BranchCache configuration is correct:
vserver cifs branchcache show -vserver vservenamer

Examples

The following commands verify that both SMB 2.1 and 3.0 are enabled and configure BranchCache to automatically enable caching on all SMB shares on SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*-> vserver cifs options show -vserver vs1 -fields smb2-enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true

cluster1::*-> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path /hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

Vserver: vs1
Supported BranchCache Versions: enable_all
Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: all_shares
```

The following commands verify that both SMB 2.1 and 3.0 are enabled, configure BranchCache to enable caching on a per-share basis on SVM vs1, and verify the BranchCache configuration:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*-> vserver cifs options show -vserver vs1 -fields smb2-enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true

cluster1::*-> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path /hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my server key"

cluster1::> vserver cifs branchcache show -vserver vs1

Vserver: vs1
Supported BranchCache Versions: enable_all
Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share
```

Related concepts

- Requirements, considerations, and recommendations on page 337
- Where to find information about configuring BranchCache at the remote office on page 343
- Managing and monitoring the BranchCache configuration on page 346
- Disabling or enabling BranchCache on the SVM on page 356
Where to find information about configuring BranchCache at the remote office

After configuring BranchCache on the CIFS server, you must install and configure BranchCache on client computers and, optionally, on caching servers at your remote office. Microsoft provides instructions for configuring BranchCache at the remote office.

Instructions for configuring branch office clients and, optionally, caching servers to use BranchCache are on the Microsoft BranchCache web site at Microsoft BranchCache: technet.microsoft.com/EN-US/NETWORK/DD425028.

Configuring BranchCache-enabled SMB shares

After you configure BranchCache on the CIFS server and at the branch office, you can enable BranchCache on SMB shares that contain content that you want to allow clients at branch offices to cache.

BranchCache caching can be enabled on all SMB shares on the CIFS server or on a share-by-share basis.

- If you enable BranchCache on a share-by-share basis, you can enable BranchCache as you create the share or by modifying existing shares.
  If you enable caching on an existing SMB share, Data ONTAP begins computing hashes and sending metadata to clients requesting content as soon as you enable BranchCache on that share.

- Any clients that have an existing SMB connection to a share do not get BranchCache support if BranchCache is subsequently enabled on that share.
  Data ONTAP advertises BranchCache support for a share at the time the SMB session is set up. Clients that already have established sessions when BranchCache is enabled need to disconnect and reconnect to use cached content for this share.

  **Note:** If BranchCache on a SMB share is subsequently disabled, Data ONTAP stops sending metadata to the requesting client. A client that needs data retrieves it directly from the content server (CIFS server).

Creating a BranchCache-enabled SMB share

You can enable BranchCache on an SMB share when you create the share by setting the `branchcache` share property.

About this task

- If BranchCache is enabled on the SMB share, the share must have the offline files configuration set to manual caching.
  This is the default setting when you create a share.

- You can also specify additional optional share parameters when you create the BranchCache-enabled share.

- You can set the `branchcache` property on a share even if BranchCache is not configured and enabled on the Storage Virtual Machine (SVM).
  However, if you want the share to offer cached content, you must configure and enable BranchCache on the SVM.
• Since there are no default share properties applied to the share when you use the -share-properties parameter, you must specify all other share properties that you want applied to the share in addition to the **branchcache** share property by using a comma-delimited list.

• For more information, see the man page for the `vserver cifs share create` command.

**Steps**

1. Create a BranchCache-enabled SMB share:

   ```bash
   vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties branchcache[,....]
   ```

   - **-path** *path* specifies the path to the share.
   - Path separators can be backward or forward slashes, although Data ONTAP displays them as forward slashes.

2. Verify that the BranchCache share property is set on the SMB share by using the `vserver cifs share show` command.

**Example**

The following command creates a BranchCache-enabled SMB share named “data” with a path of `/data` on SVM vs1. By default, the offline files setting is set to **manual**:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path /data -share-properties branchcache,oplocks,browsable,changenotify
```

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data
Vserver: vs1
Share: data
CIFS Server NetBIOS Name: VS1
Path: /data
Share Properties: branchcache
oplocks
browsable
changenotify
Symlink Properties: enable
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: data
Offline Files: manual
Vscan File-Operations Profile: standard
```

**Related tasks**

- *Creating an SMB share on a CIFS server* on page 177
- *Disabling BranchCache on a single SMB share* on page 355

**Enabling BranchCache on an existing SMB share**

You can enable BranchCache on an existing SMB share by adding the **branchcache** share property to the existing list of share properties.

**About this task**

- If BranchCache is enabled on the SMB share, the share must have the offline files configuration set to manual caching.
If the existing share’s offline files setting is not set to manual caching, you must configure it by modifying the share.

- You can set the branchcache property on a share even if BranchCache is not configured and enabled on the Storage Virtual Machine (SVM).
  However, if you want the share to offer cached content, you must configure and enable BranchCache on the SVM.

- When you add the branchcache share property to the share, existing share settings and share properties are preserved.
  The BranchCache share property is added to the existing list of share properties. For more information about using the vserver cifs share properties add command, see the man pages.

Steps

1. If necessary, configure the offline files share setting for manual caching:
   a. Determine what the offline files share setting is by using the vserver cifs share show command.
   b. If the offline files share setting is not set to manual, change it to the required value:
      
      ```
      vserver cifs share modify -vserver vs1-name -share-name share_name
      -offline-files manual
      ```

2. Enable BranchCache on an existing SMB share:

   ```
   vserver cifs share properties add -vserver vs1-name -share-name
   share_name -share-properties branchcache
   ```

3. Verify that the BranchCache share property is set on the SMB share:

   ```
   vserver cifs share show -vserver vs1-name -share-name share_name
   ```

Example

The following command enables BranchCache on an existing SMB share named “data2” with a path of /data2 on SVM vs1:

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

Vserver: vs1
  Share: data2
  CIFS Server NetBIOS Name: VS1
  Path: /data2
  Share Properties: oplocks
                  browsable
                  changenotify
                  showsnapshot
  Symlink Properties: -
  File Mode Creation Mask: -
  Directory Mode Creation Mask: -
  Share Comment: -
  Share ACL: Everyone / Full Control
  File Attribute Cache Lifetime: 10s
  Volume Name: -
  Offline Files: manual
  Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

Vserver: vs1
  Share: data2
  CIFS Server NetBIOS Name: VS1
  Path: /data2
```
Share Properties: oplocks
  browsable
  showsnapshot
  changenotify
  branchcache

Symlink Properties: -

File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control

File Attribute Cache Lifetime: 10s
Volume Name: -
Offline Files: manual
Vacan File-Operations Profile: standard

### Related tasks

*Adding or removing share properties on an existing SMB share* on page 183
*Disabling BranchCache on a single SMB share* on page 355

### Managing and monitoring the BranchCache configuration

You manage the BranchCache configuration by modifying BranchCache parameters, changing the server secret key, configuring BranchCache to pre-compute hashes, flushing the hash cache, and configuring BranchCache GPOs. You can also display information about BranchCache statistics.

### Related concepts

*Considerations when choosing the hash store location* on page 338

### Modifying BranchCache configurations

You can modify the configuration of the BranchCache service on Storage Virtual Machines (SVMs), including changing the hash store directory path, the hash store maximum directory size, the operating mode, and which BranchCache versions are supported. You can also increase the size of the volume that contains the hash store.

### Steps

1. Perform the appropriate action:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Enter the following...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify the hash store directory size</td>
<td>`vserver cifs branchcache modify -vserver vserver_name -hash-store-max-size {integer[KB</td>
</tr>
<tr>
<td>Increase the size of the volume that contains the hash store</td>
<td>`volume size -vserver vserver_name -volume volume_name -new-size new_size{k</td>
</tr>
</tbody>
</table>

   If the volume containing the hash store fills up, you might be able to increase the size of the volume. You can specify the new volume size as a number followed by a unit designation.

   See the *Clustered Data ONTAP Logical Storage Management Guide* for more information about increasing volume size.
<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Enter the following...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify the hash store directory path</td>
<td>`vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true</td>
</tr>
</tbody>
</table>

If the SVM is an SVM disaster recovery source, the hash path cannot be on the root volume. This is because the root volume is not replicated to the disaster recovery destination.

The BranchCache hash path can contain blanks and any valid file name characters.

If you modify the hash path, `-flush-hashes` is a required parameter that specifies whether you want Data ONTAP to flush the hashes from the original hash store location. You can set the following values for the `-flush-hashes` parameter:

- If you specify `true`, Data ONTAP deletes the hashes in the original location and creates new hashes in the new location as new requests are made by BranchCache-enabled clients.
- If you specify `false`, the hashes are not flushed. In this case, you can choose to reuse the existing hashes later by changing the hash store path back to the original location.

<table>
<thead>
<tr>
<th>Change the operating mode</th>
<th><code>vserver cifs branchcache modify -vserver vserver_name -operating-mode mode</code></th>
</tr>
</thead>
</table>

The possible values for `-operating-mode` are as follows:

- `per-share`
- `all-shares`
- `disable`

**Note:** You should be aware of the following when modifying the operating mode:

- Data ONTAP advertises BranchCache support for a share when the SMB session is set up.
- Clients that already have established sessions when BranchCache is enabled need to disconnect and reconnect to use cached content for this share.

| Change the BranchCache version support | `vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable|v2-enable|enable-all}` |
|---------------------------------------|--------------------------------------------------|

2. Verify the configuration changes by using the `vserver cifs branchcache show` command.

**Displaying information about BranchCache configurations**

You can display information about BranchCache configurations on Storage Virtual Machines (SVMs) with FlexVol volumes, which can be used when verifying a configuration or when determining current settings before modifying a configuration.

**Step**

1. Perform one of the following actions:
If you want to display... Enter this command...

Summary information about BranchCache configurations on all SVMs

Summary information about BranchCache configurations on all SVMs

vserver cifs branchcache show

Detailed information about the configuration on a specific SVM

Detailed information about the configuration on a specific SVM

vserver cifs branchcache show -vserver vserver_name

Example

The following example displays information about the BranchCache configuration on SVM vs1:

cluster1::> vserver cifs branchcache show -vserver vs1

Vserver: vs1
Supported BranchCache Versions: enable_all
Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share

Changing the BranchCache server key

You can change the BranchCache server key by modifying the BranchCache configuration on the Storage Virtual Machine (SVM) and specifying a different server key.

About this task

You can set the server key to a specific value so that if multiple servers are providing BranchCache data for the same files, clients can use hashes from any server using that same server key.

When you change the server key, you must also flush the hash cache. After flushing the hashes, Data ONTAP creates new hashes as new requests are made by BranchCache-enabled clients.

Steps

1. Change the server key by using the following command:

   vserver cifs branchcache modify -vserver vserver_name -server-key text -flush-hashes true

   - -server-key text specifies the text string to use as the server key.
   - If the server key contains any spaces, enclose the server key in quotation marks.
   - When configuring a new server key, you must also specify -flush-hashes and set the value to true.

2. Verify that the BranchCache configuration is correct by using the vserver cifs branchcache show command.

Example

The following example sets a new server key that contains spaces and flushes the hash cache on SVM vs1:

cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1
Pre-computing BranchCache hashes on specified paths

You can configure the BranchCache service to pre-compute hashes for a single file, for a directory, or for all files in a directory structure. This can be helpful if you want to compute hashes on data in a BranchCache-enabled share during off, non-peak hours.

Before you begin

You must use the `statistics start` and optional `statistics stop` commands if you want to collect a data sample before you display hash statistics. For more information about these commands, see the Clustered Data ONTAP System Administration Guide for Cluster Administrators.

About this task

- You must specify the Storage Virtual Machine (SVM) and path on which you want to pre-compute hashes.
- You must also specify whether you want hashes computed recursively.
- If you want hashes computed recursively, the BranchCache service traverses the entire directory tree under the specified path, and computes hashes for each eligible object.

Steps

1. Perform the appropriate command:

<table>
<thead>
<tr>
<th>If you want to pre-compute hashes on...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>A single file or directory</td>
<td><code>vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false</code></td>
</tr>
<tr>
<td>Recursively on all files in a directory structure</td>
<td><code>vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse true</code></td>
</tr>
</tbody>
</table>

- `path` is specified as an absolute path.

2. Verify that hashes are being computed by using the `statistics` command:

   a. Display statistics for the `hashd` object on the desired SVM instance:

      ```
      statistics show -object hashd -instance vserver_name
      ```

   b. Verify that the number of hashes created is increasing by repeating the command.

Examples

The following example creates hashes on the path `/data` and on all contained files and subdirectories on SVM vs1:
Flushing hashes from the SVM BranchCache hash store

You can flush all cached hashes from the BranchCache hash store on the Storage Virtual Machine (SVM). This can be useful if you have changed the branch office BranchCache configuration. For example, if you recently reconfigured the caching mode from distributed caching to hosted caching mode, you would want to flush the hash store.

**About this task**

After flushing the hashes, Data ONTAP creates new hashes as new requests are made by BranchCache-enabled clients.

**Step**

1. Flush the hashes from the BranchCache hash store:

   ```
   vserver cifs branchcache hash-flush -vserver vserver_name
   ```

   **Example**

   ```
   vserver cifs branchcache hash-flush -vserver vs1
   ```
Displaying BranchCache statistics

You can display BranchCache statistics to, among other things, identify how well caching is performing, determine whether your configuration is providing cached content to clients, and determine whether hash files were deleted to make room for more recent hash data.

About this task

The `hashd` statistic object contains counters that provide statistical information about BranchCache hashes. The `cifs` statistic object contains counters that provide statistical information about BranchCache-related activity. You can collect and display information about these objects at the advanced-privilege level.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

   Example

   ```
   cluster1::> set -privilege advanced
   Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.
   Do you want to continue? {y|n}: y
   ```

2. Display the BranchCache-related counters by using the statistics catalog counter show command.

   For more information about statistics counters, see the man page for this command.

   Example

   ```
   cluster1::*> statistics catalog counter show -object hashd
   Object: hashd
   Counter                     Description
   --------------------------- ----------------------------------------------
   branchcache_hash_created    Number of times a request to generate BranchCache hash for a file succeeded.
   branchcache_hash_files_replaced
   Number of times a BranchCache hash file was deleted to make room for more recent hash data. This happens if the hash store size is exceeded.
   branchcache_hash_rejected   Number of times a request to generate BranchCache hash data failed.
   branchcache_hash_store_bytes
   Total number of bytes used to store hash data.
   branchcache_hash_store_size
   Total space used to store BranchCache hash data for the Vserver.
   instance_name               Instance Name
   instance_uuid               Instance UUID
   node_name                   System node name
   node_uuid                   System node id
   9 entries were displayed.
   ```

   ```
   cluster1::*> statistics catalog counter show -object cifs
   Object: cifs
   Counter                     Description
   --------------------------- ----------------------------------------------
   active_searches             Number of active searches over SMB and SMB2
   auth_reject_too_many        Authentication refused after too many requests were made in rapid succession
   avg_directory_depth         Average number of directories crossed by SMB and SMB2 path-based commands
   ```
<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>avg_junction_depth</td>
<td>Average number of junctions crossed by SMB and SMB2 path-based commands</td>
</tr>
<tr>
<td>branchcache_hash_fetch_fail</td>
<td>Total number of times a request to fetch hash data failed. These are failures when attempting to read existing hash data. It does not include attempts to fetch hash data that has not yet been generated.</td>
</tr>
<tr>
<td>branchcache_hash_fetch_ok</td>
<td>Total number of times a request to fetch hash data succeeded.</td>
</tr>
<tr>
<td>branchcache_hash_sent_bytes</td>
<td>Total number of bytes sent to clients requesting hashes.</td>
</tr>
<tr>
<td>branchcache_missing_hash_bytes</td>
<td>Total number of bytes of data that had to be read by the client because the hash for that content was not available on the server.</td>
</tr>
</tbody>
</table>

3. **Collect BranchCache-related statistics by using the `statistics start` and `statistics stop` commands.**

For more information about collecting statistics, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

**Example**

```
cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11
```

4. **Display the collected BranchCache statistics by using the `statistics show` command.**

For more information about displaying statistical information, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

**Example**

```
cluster1::*> statistics show -object cifs -counter branchcache_hash_sent_bytes -sample-id 11
Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1
                      Value
------------------- ---------------------------------
branchcache_hash_sent_bytes                  0
branchcache_hash_sent_bytes                  0
branchcache_hash_sent_bytes                  0
branchcache_hash_sent_bytes                  0

cluster1::*> statistics show -object cifs -counter branchcache_missing_hash_bytes -sample-id 11
Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1
                      Value
------------------- ---------------------------------
branchcache_missing_hash_bytes                0
branchcache_missing_hash_bytes                0
branchcache_missing_hash_bytes                0
branchcache_missing_hash_bytes                0
```

5. **Return to the admin privilege level:**

```
set -privilege admin
```
Support for BranchCache Group Policy Objects

Data ONTAP BranchCache provides support for BranchCache Group Policy Objects (GPOs), which allow centralized management for certain BranchCache configuration parameters. There are two GPOs used for BranchCache, the Hash Publication for BranchCache GPO and the Hash Version Support for BranchCache GPO.

Hash Publication for BranchCache GPO

The Hash Publication for BranchCache GPO corresponds to the \textit{-operating-mode} parameter. When GPO updates occur, this value is applied to Storage Virtual Machine (SVM) objects contained within the organizational unit (OU) to which the group policy applies.

Hash Version Support for BranchCache GPO

The Hash Version Support for BranchCache GPO corresponds to the \textit{-versions} parameter. When GPO updates occur, this value is applied to SVM objects contained within the organizational unit to which the group policy applies.

Related concepts

\textit{Applying Group Policy Objects to CIFS servers} on page 113

Displaying information about BranchCache Group Policy Objects

You can display information about the CIFS server's Group Policy Object (GPO) configuration to determine whether BranchCache GPOs are defined for the domain to which the CIFS server belongs and, if so, what the allowed settings are. You can also determine whether BranchCache GPO settings are applied to the CIFS server.

About this task

Even though a GPO setting is defined within the domain to which the CIFS server belongs, it is not necessarily applied to the organizational unit (OU) containing the CIFS-enabled Storage Virtual Machine (SVM). Applied GPO setting are the subset of all defined GPOs that are applied to the CIFS-enabled SVM. BranchCache settings applied through GPOs override settings applied through the CLI.

Steps

1. Display the defined BranchCache GPO setting for the Active Directory domain by using the \texttt{vserver cifs group-policy show-defined} command.

Example

\textbf{Note:} This example does not display all of the available output fields for the command. Output is truncated.

\begin{verbatim}
cluster1:> vserver cifs group-policy show-defined -vserver vs1
Vserver: vs1
------------------------
GPO Name: Default Domain Policy
\end{verbatim}
2. Display the BranchCache GPO setting applied to the CIFS server by using the `vserver cifs group-policy show-applied` command.

    Example
    
    Note: This example does not display all of the available output fields for the command. Output is truncated.

    ```
    cluster1::> vserver cifs group-policy show-applied -vserver vs1
    Vserver: vs1
    -----------------------------------------------
    GPO Name: Default Domain Policy
    Level: Domain
    Status: enabled
    Advanced Audit Settings:
    Object Access:
    Central Access Policy Staging: failure
    Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: version1
    [...] 
    GPO Name: Resultant Set of Policy
    Level: RSOP
    Status: enabled
    Advanced Audit Settings:
    Object Access:
    Central Access Policy Staging: failure
    Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: version1
    [...] 
    ```

    Related tasks
    
    * Enabling or disabling GPO support on a CIFS server on page 118

### Disabling BranchCache on SMB shares

If you do not want to provide BranchCache caching services on certain SMB shares but you might want to provide caching services on those shares later, you can disable BranchCache on a share-by-share basis. If you have BranchCache configured to offer caching on all shares but you want to
temporarily disable all caching services, you can modify the BranchCache configuration to stop automatic caching on all shares.

If BranchCache on an SMB share is subsequently disabled after first being enabled, Data ONTAP stops sending metadata to the requesting client. A client that needs data retrieves it directly from the content server (CIFS server on the Storage Virtual Machine (SVM)).

**Related concepts**

*Configuring BranchCache-enabled SMB shares* on page 343

**Disabling BranchCache on a single SMB share**

If you do not want to offer caching services on certain shares that previously offered cached content, you can disable BranchCache on an existing SMB share.

**Step**

1. Enter the following command:

   ```
   vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties branchcache
   ```

   The BranchCache share property is removed. Other applied share properties remain in effect.

**Example**

The following command disables BranchCache on an existing SMB share named “data2”:

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2
   
   Vserver: vs1
   Share: data2
   CIFS Server NetBIOS Name: VS1
   Path: /data2
   Share Properties: oplocks
                     browsable
                     changenotify
                     attributecache
                     branchcache
   
   Symlink Properties: -
   File Mode Creation Mask: -
   Directory Mode Creation Mask: -
   Share Comment: -
   Share ACL: Everyone / Full Control
   File Attribute Cache Lifetime: 10s
   Volume Name: -
   Offline Files: manual
   Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name data2 -share-properties branchcache
```

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2
   
   Vserver: vs1
   Share: data2
   CIFS Server NetBIOS Name: VS1
   Path: /data2
   Share Properties: oplocks
                     browsable
                     changenotify
                     attributecache
   
   Symlink Properties: -
   File Mode Creation Mask: -
   Directory Mode Creation Mask: -
   Share Comment: -
   Share ACL: Everyone / Full Control
```
Stopping automatic caching on all SMB shares

If your BranchCache configuration automatically enables caching on all SMB shares on each Storage Virtual Machine (SVM) with FlexVol volumes, you can modify the BranchCache configuration to stop automatically caching content for all SMB shares.

About this task

To stop automatic caching on all SMB shares, you change the BranchCache operating mode to per-share caching.

Steps

1. Configure BranchCache to stop automatic caching on all SMB shares by entering the following command:

   vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share

2. Verify that the BranchCache configuration is correct:

   vserver cifs branchcache show -vserver vserver_name

Example

The following command changes the BranchCache configuration on Storage Virtual Machine (SVM, formerly known as Vserver) vs1 to stop automatic caching on all SMB shares:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode per-share
cluster1::> vserver cifs branchcache show -vserver vs1
```

<table>
<thead>
<tr>
<th>Vserver: vs1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported BranchCache Versions: enable_all</td>
</tr>
<tr>
<td>Path to Hash Store: /hash_data</td>
</tr>
<tr>
<td>Maximum Size of the Hash Store: 20GB</td>
</tr>
<tr>
<td>Encryption Key Used to Secure the Hashes: -</td>
</tr>
<tr>
<td>CIFS BranchCache Operating Modes: per_share</td>
</tr>
</tbody>
</table>

Disabling or enabling BranchCache on the SVM

You can disable BranchCache on the Storage Virtual Machine (SVM) if you temporarily do not want to offer caching services on that SVM. You can easily offer caching services again in the future by enabling BranchCache on the SVM.

What happens when you disable or reenable BranchCache on the CIFS server

If you previously configured BranchCache but do not want the branch office clients to use cached content, you can disable caching on the CIFS server. You must be aware of what happens when you disable BranchCache.

When you disable BranchCache, Data ONTAP no longer computes hashes or sends the metadata to the requesting client. However, there is no interruption to file access. Thereafter, when BranchCache-enabled clients request metadata information for content they want to access, Data ONTAP responds with a Microsoft-defined error, which causes the client to send a second request, requesting the actual...
content. In response to the request for content, the CIFS server sends the actual content that is stored on the Storage Virtual Machine (SVM).

After BranchCache is disabled on the CIFS server, SMB shares do not advertise BranchCache capabilities. To access data on new SMB connections, clients make normal read SMB requests.

You can reenable BranchCache on the CIFS server at any time.

- Because the hash store is not deleted when you disable BranchCache, Data ONTAP can use the stored hashes when replying to hash requests after you reenable BranchCache, provided that the requested hash is still valid.
- Any clients that have made SMB connections to BranchCache-enabled shares during the time when BranchCache was disabled do not get BranchCache support if BranchCache is subsequently reenabled.

This is because Data ONTAP advertises BranchCache support for a share at the time the SMB session is set up. Clients that established sessions to BranchCache-enabled shares while BranchCache was disabled need to disconnect and reconnect to use cached content for this share.

**Note:** If you do not want to save the hash store after you disable BranchCache on a CIFS server, you can manually delete it. If you reenable BranchCache, you must ensure that the hash store directory exists. After BranchCache is reenabled, BranchCache-enabled shares advertise BranchCache capabilities. Data ONTAP creates new hashes as new requests are made by BranchCache-enabled clients.

### Disabling or enabling BranchCache

You can disable BranchCache on the Storage Virtual Machine (SVM) with FlexVol volumes by changing the BranchCache operating mode to `disabled`. You can enable BranchCache at any time by changing the operating mode to either offer BranchCache services per-share or automatically for all shares.

#### Steps

1. Run the appropriate command:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Then enter the following...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable BranchCache</td>
<td><code>vserver cifs branchcache modify -vserver vserver_name -operating-mode disable</code></td>
</tr>
<tr>
<td>Enable BranchCache per share</td>
<td><code>vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share</code></td>
</tr>
<tr>
<td>Enable BranchCache for all shares</td>
<td><code>vserver cifs branchcache modify -vserver vserver_name -operating-mode all-shares</code></td>
</tr>
</tbody>
</table>

2. Verify that the BranchCache operating mode is configured with the desired setting:

`vserver cifs branchcache show -vserver vserver_name`
Deleting the BranchCache configuration on SVMs

You can delete the BranchCache configuration if you no longer want to offer caching services on that Storage Virtual Machine (SVM).

What happens when you delete the BranchCache configuration

If you previously configured BranchCache but do not want the Storage Virtual Machine (SVM) to continue providing cached content, you can delete the BranchCache configuration on the CIFS server. You must be aware of what happens when you delete the configuration.

When you delete the configuration, Data ONTAP removes the configuration information for that SVM from the cluster and stops the BranchCache service. You can choose whether Data ONTAP should delete the hash store on the SVM.

Deleting the BranchCache configuration does not disrupt access by BranchCache-enabled clients. Thereafter, when BranchCache-enabled clients request metadata information on existing SMB connections for content that is already cached, Data ONTAP responds with a Microsoft defined error, which causes the client to send a second request, requesting the actual content. In response to the request for content, the CIFS server sends the actual content that is stored on the SVM.

After the BranchCache configuration is deleted, SMB shares do not advertise BranchCache capabilities. To access content that has not previously been cached using new SMB connections, clients make normal read SMB requests.

Deleting the BranchCache configuration

The command you use for deleting the BranchCache service on your Storage Virtual Machine (SVM) differs depending on whether you want to delete or keep existing hashes.

Step

1. Run the appropriate command:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Then enter the following...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete the BranchCache configuration and delete existing hashes</td>
<td><code>vserver cifs branchcache delete -vserver vserver_name -flush-hashes true</code></td>
</tr>
<tr>
<td>Delete the BranchCache configuration but keep existing hashes</td>
<td><code>vserver cifs branchcache delete -vserver vserver_name -flush-hashes false</code></td>
</tr>
</tbody>
</table>

Example

The following example deletes the BranchCache configuration on SVM vs1 and deletes all existing hashes:

`cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes true`
What happens to BranchCache when reverting

It is important to understand what happens when you revert Data ONTAP to a release that does not support BranchCache.

• When you revert to a version of Data ONTAP that does not support BranchCache, the SMB shares do not advertise BranchCache capabilities to BranchCache-enabled clients; therefore, the clients do not request hash information. Instead, they request the actual content using normal SMB read requests. In response to the request for content, the CIFS server sends the actual content that is stored on the Storage Virtual Machine (SVM).

• When a node hosting a hash store is reverted to a release that does not support BranchCache, the storage administrator needs to manually revert the BranchCache configuration using a command that is printed out during the revert. This command deletes the BranchCache configuration and hashes. After the revert completes, the storage administrator can manually delete the directory that contained the hash store if desired.

Related concepts

Deleting the BranchCache configuration on SVMs on page 358

Improving Microsoft remote copy performance

Microsoft Offloaded Data Transfer (ODX), also known as copy offload, enables direct data transfers within or between compatible storage devices without transferring the data through the host computer.

Data ONTAP supports ODX for both the SMB and SAN protocols. The source can be either a CIFS server or LUN, and the destination can be either a CIFS server or LUN.

In non-ODX file transfers, the data is read from the source and is transferred across the network to the client computer. The client computer transfers the data back over the network to the destination. In summary, the client computer reads the data from the source and writes it to the destination. With ODX file transfers, data is copied directly from the source to the destination.

Because ODX offloaded copies are performed directly between the source and destination storage, there are significant performance benefits. The performance benefits realized include faster copy time between source and destination, reduced resource utilization (CPU, memory) on the client, and reduced network I/O bandwidth utilization.

For SMB environments, this functionality is only available when both the client and the storage server support SMB 3.0 and the ODX feature. For SAN environments, this functionality is only available when both the client and the storage server support the ODX feature. Client computers that support ODX and have ODX enabled automatically and transparently use offloaded file transfer when moving or copying files. ODX is used irrespective of whether you drag-and-drop files through Windows Explorer or use command-line file copy commands, or whether a client application initiates file copy requests.

Related concepts

Improving client response time by providing SMB automatic node referrals with Auto Location on page 364
How ODX copy offload is used with Hyper-V and SQL Server over SMB shares on page 381
How ODX works

ODX copy offload uses a token-based mechanism for reading and writing data within or between ODX-enabled CIFS servers. Instead of routing the data through the host, the CIFS server sends a small token, which represents the data, to the client. The ODX client presents that token to the destination server, which then can transfer the data represented by that token from the source to the destination.

When an ODX client learns that the CIFS server is ODX-capable, it opens the source file and requests a token from the CIFS server. After opening the destination file, the client uses the token to instruct the server to copy the data directly from the source to the destination.

**Note:** The source and destination can be on the same Storage Virtual Machine (SVM) or on different SVMs, depending on the scope of the copy operation.

The token serves as a point-in-time representation of the data. As an example, when you copy data between storage locations, a token representing a data segment is returned to the requesting client, which the client copies to the destination, thereby removing the need to copy the underlying data through the client.

Data ONTAP supports tokens that represent 8 MB of data. ODX copies of greater than 8 MB are performed by using multiple tokens, with each token representing 8 MB of data.

The following figure explains the steps that are involved with an ODX copy operation:

1. A user copies or moves a file by using Windows Explorer, a command-line interface, or as part of a virtual machine migration, or an application initiates file copies or moves.
2. The ODX-capable client automatically translates this transfer request into an ODX request.
The ODX request that is sent to the CIFS server contains a request for a token.

3. If ODX is enabled on the CIFS server and the connection is over SMB 3.0, the CIFS server generates a token, which is a logical representation of the data on the source.

4. The client receives a token that represents the data and sends it with the write request to the destination CIFS server.
   This is the only data that is copied over the network from the source to the client and then from the client to the destination.

5. The token is delivered to the storage subsystem.

6. The SVM internally performs the copy or move.
   If the file that is copied or moved is larger than 8 MB, multiple tokens are needed to perform the copy. Steps 2 through 6 as performed as needed to complete the copy.

   **Note:** If there is a failure with the ODX offloaded copy, the copy or move operation falls back to traditional reads and writes for the copy or move operation. Similarly, if the destination CIFS server does not support ODX or ODX is disabled, the copy or move operation falls back to traditional reads and writes for the copy or move operation.

**Requirements for using ODX**

Before you can use ODX for copy offloads with your Storage Virtual Machine (SVM) with FlexVol volumes, you need to be aware of certain requirements.

**Data ONTAP version requirements**

Clustered Data ONTAP 8.2 and later releases support ODX for copy offloads.

**SMB version requirements**

- Clustered Data ONTAP supports ODX with SMB 3.0 and later.
- SMB 3.0 must be enabled on the CIFS server before ODX can be enabled:
  - Enabling ODX also enables SMB 3.0, if it is not already enabled.
  - Disabling SMB 3.0 also disables ODX.

**Windows server and client requirements**

Before a user can use ODX for copy offloads, the Windows client must support the feature. Support for ODX starts with Windows 2012 Server and Windows 8.

For the latest information about which Windows clients support ODX, see the Interoperability Matrix at [mysupport.netapp.com/matrix](http://mysupport.netapp.com/matrix).

**Volume requirements**

- Source volumes must be a minimum of 1.25 GB.
- Deduplication must be enabled on volumes used with copy offload.
- Compression must *not* be enabled on volumes used with copy offload.
Considerations for using ODX

Before you can use ODX for copy offload, you need to be aware of certain considerations. For example, you need to know on which types of volumes you can use ODX and you need to understand the intra-cluster and inter-cluster ODX considerations.

Volume considerations

• You cannot use ODX for copy offload with the following volume configurations:
  ◦ Source volume size is less than 1.25 GB
    The volume size must be 1.25 GB or larger to use ODX.
  ◦ Read-only volumes
    ODX is not used for files and folders residing in load-sharing mirrors or in SnapMirror or SnapVault destination volumes.
  ◦ If the source volume is compressed
  ◦ If the source volume is not deduplicated

• ODX copies are supported only for intra-cluster copies.
  You cannot use ODX to copy files or folders to a volume in another cluster.

• ODX is supported for Storage Virtual Machines (SVMs) with FlexVol volumes.
  You cannot use ODX to copy data to or from volumes in SVMs with Infinite Volume.

Other considerations

• In SMB environments, to use ODX for copy offload, the files must be 256 kb or larger.
  Smaller files are transferred using a traditional copy operation.

• ODX copy offload uses deduplication as part of the copy process.
  If you do not want deduplication to occur on SVM volumes when copying or moving data, you should disable ODX copy offload on that SVM.

• The application that performs the data transfer must be written to support ODX.
  Application operations that support ODX include the following:
    ◦ Hyper-V management operations, such as creating and converting virtual hard disks (VHDs), managing Snapshot copies, and copying files between virtual machines
    ◦ Windows Explorer operations
    ◦ Windows PowerShell copy commands
    ◦ Windows command prompt copy commands
    ◦ Robocopy at the Windows command prompt supports ODX.

  Note: The applications must be running on Windows servers or clients that support ODX.
  For more information about supported ODX applications on Windows servers and clients, consult the Microsoft TechNet Library.

Related information

Use cases for ODX

You should be aware of the use cases for using ODX on SVMs with FlexVol volumes so that you can determine under what circumstances this feature provides you with performance benefits.

Windows servers and clients that support ODX use copy offload as the default way of copying data across remote servers. If the Windows server or client does not support ODX or the ODX copy offload fails at any point, the copy or move operation falls back to traditional reads and writes for the copy or move operation.

The following use cases support using ODX copies and moves:

• Intra-volume
  The source and destination files or LUNs are within the same volume.

• Inter-volume, same node, same SVM
  The source and destination files or LUNs are on different volumes that are located on the same node. The data is owned by the same SVM.

• Inter-volume, different nodes, same SVM
  The source and destination files or LUNs are on different volumes that are located on different nodes. The data is owned by the same SVM.

• Inter-SVM, same node
  The source and destination file or LUNs are on different volumes that are located on the same node. The data is owned by different SVMs.

• Inter-SVM, different nodes
  The source and destination file or LUNs are on different volumes that are located on different nodes. The data is owned by different SVMs.

There are some additional special use cases:

• With the Data ONTAP ODX implementation, you can use ODX to copy files between SMB shares and FC or iSCSI attached virtual drives.
  You can use Windows Explorer, the Windows CLI or PowerShell, Hyper-V, or other applications that support ODX to copy or move files seamlessly using ODX copy offload between SMB shares and connected LUNs, provided the SMB shares and LUNs are on the same cluster.

• Hyper-V provides some additional use cases for ODX copy offload:
  ◦ You can use ODX copy offload pass-through with Hyper-V to copy data within or across virtual hard disk (VHD) files or to copy data between mapped SMB shares and connected iSCSI LUNs within the same cluster.
    This allows copies from guest operating systems to pass through to the underlying storage.
  ◦ When creating fixed-sized VHDs, ODX is used for initializing the disk with zeros, using a well-known zeroed token.
  ◦ ODX copy offload is used for virtual machine storage migration if the source and destination storage is on the same cluster.

Note: To take advantage of the use cases for ODX copy offload pass-through with Hyper-V, the guest operating system must support ODX and the guest operating system’s disks must be SCSI disks backed by storage (either SMB or SAN) that supports ODX. IDE disks on the guest operating system do not support ODX pass-through.
Enabling or disabling ODX

You can enable or disable ODX on Storage Virtual Machines (SVMs) with FlexVol volumes. The default is to enable support for ODX copy offload if SMB 3.0 is also enabled.

Before you begin
SMB 3.0 must be enabled.

About this task
If you disable SMB 3.0, Data ONTAP also disables SMB ODX. If you reenable SMB 3.0, you must manually reenable SMB ODX.

Steps
1. Set the privilege level to advanced:
   ```
   set -privilege advanced
   ```
2. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want ODX copy offload to be...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>vserver cifs options modify -vserver vserver_name -copy-offload-enabled true</td>
</tr>
<tr>
<td>Disabled</td>
<td>vserver cifs options modify -vserver vserver_name -copy-offload-enabled false</td>
</tr>
</tbody>
</table>
3. Return to the admin privilege level:
   ```
   set -privilege admin
   ```

Example
The following example enables ODX copy offload on SVM vs1:

```bash
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y
cluster1::*:> vserver cifs options modify -vserver vs1 -copy-offload-enabled true
cluster1::*:> set -privilege admin
```

Related references
Available CIFS server options on page 70

Improving client response time by providing SMB automatic node referrals with Auto Location

Auto Location uses SMB automatic node referrals to increase SMB client performance on Storage Virtual Machines (SVMs) with FlexVol volumes. Automatic node referrals automatically redirect the
requesting client to a LIF on the node SVM that is hosting the FlexVol volume in which the data resides, which can lead to improved client response times.

When an SMB client connects to an SMB share hosted on the SVM, it might connect using a LIF that is on a node that does not own the requested data. The node to which the client is connected accesses data owned by another node by using the cluster network. The client can experience faster response times if the SMB connection uses a LIF located on the node containing the requested data:

- Data ONTAP provides this functionality by using Microsoft DFS referrals to inform SMB clients that a requested file or folder in the namespace is hosted somewhere else. A node makes a referral when it determines that there is an SVM LIF on the node containing the data.
- Automatic node referrals are supported for IPv4 and IPv6 LIF IP addresses.
- Referrals are made based on the location of the root of the share through which the client is connected.
- The referral occurs during SMB negotiation. The referral is made before the connection is established. After Data ONTAP refers the SMB client to the target node, the connection is made, and the client accesses data through the referred LIF path from that point on. This allows the clients faster access to the data and avoids extra cluster communication.

  **Note:** If a share spans multiple junction points and some of the junctions are to volumes contained on other nodes, data within the share is spread across multiple nodes. Because Data ONTAP provides referrals that are local to the root of the share, Data ONTAP must use the cluster network to retrieve the data contained within these non-local volumes.

  With this type of namespace architecture, automatic node referrals might not provide significant performance benefits.

If the node hosting the data does not have an available LIF, Data ONTAP establishes the connection using the LIF chosen by the client. After a file is opened by an SMB client, it continues to access the file through the same referred connection.

If, for any reason, the CIFS server cannot make a referral, there is no disruption to SMB service. The SMB connection is established as if automatic node referrals were not enabled.

**Related concepts**

*Improving Microsoft remote copy performance* on page 359

**Requirements and considerations when using automatic node referrals**

Before you can use SMB automatic node referrals, also known as *autolocation*, you need to be aware of certain requirements, including which versions of Data ONTAP support the feature. You also need to know about supported SMB protocol versions and certain other special considerations.

**Data ONTAP version and license requirements**

- Data ONTAP 8.2 and later releases support SMB automatic node referrals.
- All nodes in the cluster must be running a version of Data ONTAP that supports automatic node referrals.
- CIFS must be licensed, and a CIFS server must exist on the Storage Virtual Machine (SVM).
**SMB protocol version requirements**

- For SVMs with FlexVol volumes, Data ONTAP supports automatic node referrals on all versions of SMB.
- For SVMs with Infinite Volume, Data ONTAP supports automatic node referrals on SMB 1.0.

**SMB client requirements**

All Microsoft clients supported by Data ONTAP support SMB automatic node referrals.

For the latest information about which Windows clients Data ONTAP supports, see the Interoperability Matrix at [mysupport.netapp.com/matrix](https://mysupport.netapp.com/matrix).

**Data LIF requirements**

If you want to use a data LIF as a potential referral for CIFS clients, you must create data LIFs with both NFS and CIFS enabled.

Automatic node referrals can fail to work if the target node contains data LIFs that are enabled only for the NFS protocol, or enabled only for the CIFS protocol.

If this requirement is not met, data access is not affected. The SMB client maps the share using the original LIF that the client used to connect to the SVM.

**NTLM authentication requirements when making a referred SMB connection**

NTLM authentication must be allowed on the domain containing the CIFS server and on the domains containing clients that want to use automatic node referrals.

When making a referral, the CIFS server refers an IP address to the Windows client. Because NTLM authentication is used when making a connection using an IP address, Kerberos authentication is not performed for referred connections.

This happens because the Windows client cannot craft the service principal name used by Kerberos (which is of the form `service/NetBIOS name` and `service/FQDN`), which means the client cannot request a Kerberos ticket to the service.

**Considerations when using automatic node referrals with the home directory feature**

When shares are configured with the home directory share property enabled, there can be one or more home directory search paths configured for a home directory configuration. The search paths can point to volumes contained on each node containing SVM volumes. Clients receive a referral and, if an active, local data LIF is available, connect through a referred LIF that is local to the home user's home directory.

There are considerations when SMB 1.0 clients access dynamic home directories with automatic node referrals enabled. This is because SMB 1.0 clients require the automatic node referral before they have authenticated, thus, before the CIFS server has the user's name. However, CIFS home directory access works correctly for SMB 1.0 clients if the following are true:

- CIFS home directories are configured to use simple names such as “%w” (Windows user name), or “%u” (mapped UNIX user name) and not domain-name style names “%d%w” (domain-name \user-name).
- When creating home directory shares, the CIFS home directory shares names are configured with variables (“%w” or “%u”) and not with static names such as “HOME”.

For SMB 2.x and SMB 3.0 clients, there are no special considerations when accessing home directories using automatic node referrals.
Considerations when disabling automatic node referrals on CIFS servers with existing referred connections

If you disable automatic node referrals after the option has been enabled, clients currently connected to a referred LIF keep the referred connection. Because Data ONTAP uses DFS referrals as the mechanism for SMB automatic node referrals, clients can even reconnect to the referred LIF after you disable the option until the client's cached DFS referral for the referred connection times out. This is true even in the case of a revert to a version of Data ONTAP that does not support automatic node referrals. Clients continue to use referrals until the DFS referral times out from the client's cache.

Considerations when using automatic node referrals with Mac OS clients

Mac OS X clients do not support SMB automatic node referrals, even though the Mac OS supports Microsoft's Distributed File System (DFS). Windows clients make a DFS referral request before connecting to an SMB share. Clustered Data ONTAP provides a referral to a data LIF found on the same node that hosts the requested data, which leads to improved client response times. Although the Mac OS supports DFS, Mac OS clients do not behave exactly like Windows clients in this area.

Related concepts

*Managing home directories* on page 319

Related information

*Clustered Data ONTAP 8.3 Network Management Guide*

*NetApp Interoperability*

Support for automatic node referrals

Before you enable automatic node referrals, you should be aware that certain Data ONTAP functionality does not support referrals.

- The following types of volumes do not support automatic node referrals:
  - Read-only members of a load-sharing mirror
  - Destination volume of a data-protection mirror
- Node referrals do not move alongside a LIF move.
  If a client is using a referred connection over an SMB 2.x or SMB 3.0 connection and a data LIF moves nondisruptively, the client continues to use the same referred connection, even if the LIF is no longer local to the data.
- Node referrals do not move alongside a volume move.
  If a client is using a referred connection over any SMB connection and a volume move occurs, the client continues to use the same referred connection, even if the volume is no longer located on the same node as the data LIF.
- Node referrals are not supported on Storage Virtual Machines (SVMs) containing Hyper-V over SMB configurations.
  You must not enable automatic node referrals if you want to use the Witness protocol for faster nondisruptive failover with Hyper-V over SMB solutions.
Enabling or disabling SMB automatic node referrals

You can enable SMB automatic node referrals to increase SMB client access performance. You can disable automatic node referrals if you do not want Data ONTAP to make referrals to SMB clients.

Before you begin

A CIFS server must be configured and running on the Storage Virtual Machine (SVM) with FlexVol volumes.

About this task

Automatic node referrals are enabled and disabled on SVM basis. The functionality is disabled by default. Automatic node referrals are not supported on SVMs containing Hyper-V over SMB configurations. You must set the option to false if the SVM hosts Hyper-V over SMB configurations.

This option is available at the advanced privilege level.

Steps

1. Set the privilege level to advanced:
   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want SMB node automatic referrals to be...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>vserver cifs options modify -vserver vserver_name -is-referral-enabled true</td>
</tr>
<tr>
<td>Disabled</td>
<td>vserver cifs options modify -vserver vserver_name -is-referral-enabled false</td>
</tr>
</tbody>
</table>

   The option setting takes effect for new SMB sessions. Clients with existing connection can utilize node referral only when their existing cache timeout expires.

3. Return to the admin privilege level:
   ```
   set -privilege admin
   ```

Related references

Available CIFS server options on page 70

Using statistics to monitor automatic node referral activity

To determine how many SMB connections are referred, you can monitor automatic node referral activity by using the statistics command. By monitoring referrals you can determine the extent to which automatic referrals are locating connections on nodes that host the shares and whether you should redistribute your data LIFs to provide better local access to shares on the CIFS server.

About this task

The cifs object provides several counters at the advanced privilege level that are helpful when monitoring SMB automatic node referrals:

- **node_referral_issued**
  Number of clients that have been issued a referral to the share root's node after the client connected using a LIF hosted by a node different from the share root's node.
• **node_referral_local**  
  Number of clients that connected using a LIF hosted by the same node that hosts the share root. Local access generally provides optimal performance.

• **node_referral_not_possible**  
  Number of clients that have not been issued a referral to the node hosting the share root after connecting using a LIF hosted by a node different from the share root's node. This is because an active data LIF for the share root's node was not found.

• **node_referral_remote**  
  Number of clients that connected using a LIF hosted by a node different from the node that hosts the share root. Remote access might result in degraded performance.

You can monitor automatic node referral statistics on your Storage Virtual Machine (SVM) by collecting and viewing data for a specific time period (a sample). You can view data from the sample if you do not stop data collection. Stopping data collection gives you a fixed sample. Not stopping data collection gives you the ability to get updated data that you can use to compare against previous queries. The comparison can help you identify performance trends.

**Note:** To evaluate and use the information you gather from the `statistics` command, you should understand the distribution of clients in your environments.

For more information about using the `statistics` command, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators.*

**Steps**

1. Set the privilege level to advanced:
   
   `set -privilege advanced`

2. View automatic node referral statistics by using the `statistics` command.

**Example**

This example views automatic node referral statistics by collecting and viewing data for a sampled time period:

a. Start the collection:

   `statistics start -object cifs -instance vs1 -sample-id sample1`

   Statistics collection is being started for Sample-id: sample1

b. Wait for the desired collection time to elapse.

c. Stop the collection:

   `statistics stop -sample-id sample1`

   Statistics collection is being stopped for Sample-id: sample1

d. View the automatic node referral statistics:

   `statistics show -sample-id sample1 -counter *node*`

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Output displays counters for all nodes participating in SVM vs1. For clarity, only output fields related to automatic node referral statistics are provided in the example.

3. Return to the admin privilege level:
   ```
   set -privilege admin
   ```

Related tasks

*Displaying statistics* on page 305

How to monitor client-side SMB automatic node referral information using a Windows client

To determine what referrals are made from the client's perspective, you can use the Windows `dfsutil.exe` utility.

The Remote Server Administration Tools (RSAT) kit available with Windows 7 and later clients contains the `dfsutil.exe` utility. Using this utility, you can display information about the contents of the referral cache as well as view information about each referral that the client is currently using. You can also use the utility to clear the client's referral cache. For more information, consult the Microsoft TechNet Library.

Related information


Providing folder security on shares with access-based enumeration

When access-based enumeration (ABE) is enabled on an SMB share, users who do not have permission to access a folder or file contained within the share (whether through individual or group permission restrictions) do not see that shared resource displayed in their environment.

Conventional share properties allow you to specify which users (individually or in groups) have permission to view or modify files or folders contained within the share. However, they do not allow you to control whether folders or files within the share are visible to users who do not have permission to access them. This could pose problems if the names of these folders or files within the share describe sensitive information, such as the names of customers or products under development.

Access-based enumeration (ABE) extends share properties to include the enumeration of files and folders within the share. ABE therefore enables you to filter the display of files and folders within the share based on user access rights. In addition to protecting sensitive information in your workplace, ABE enables you to simplify the display of large directory structures for the benefit of users who do not need access to your full range of content.
Enabling or disabling access-based enumeration on SMB shares

You can enable or disable access-based enumeration (ABE) on SMB shares to allow or prevent users from seeing shared resources that they do not have permission to access.

About this task

By default, ABE is disabled.

Steps

1. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable ABE on a new share</td>
<td><code>vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access-based-enumeration</code></td>
</tr>
</tbody>
</table>

   `path` specifies the path to the share. Path separators can be backward or forward slashes, although Data ONTAP displays them as forward slashes.

   You can specify additional optional share settings and additional share properties when you create an SMB share. For more information, see the man page for the `vserver cifs share create` command.

| Enable ABE on an existing share | `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` |

   Existing share properties are preserved. The ABE share property is added to the existing list of share properties.

| Disable ABE on an existing share | `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` |

   Other share properties are preserved. Only the ABE share property is removed from the list of share properties.

2. Verify that the share configuration is correct by using the `vserver cifs share show` command.

Examples

The following example creates an ABE SMB share named “sales” with a path of `/sales` on Storage Virtual Machine (SVM, formerly known as Vserver) vs1. The share is created with `access-based-enumeration` as a share property:

```bash
cluster1::> vserver cifs share create -vserver vs1 -share-name sales -path /sales -share-properties access-based-enumeration,oplocks,browsable,changenotify
cluster1::> vserver cifs share show -vserver vs1 -share-name sales

Vserver: vs1
Share: sales
CIFS Server NetBIOS Name: VS1
Path: /sales
Share Properties: access-based-enumeration
                  oplocks
                  browsable
                  changenotify
Symlink Properties: enable
File Mode Creation Mask: -
Directory Mode Creation Mask: -
```
The following example adds the **access-based-enumeration** share property to an SMB share named “data2”:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name data2 -share-properties access-based-enumeration
```

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2 -fields server share-name share-properties

server  share-name share-properties
------- ---------- -------------------------------------------------------
vs1      data2      oplocks,browsable,changenotify,access-based-enumeration
```

**Related tasks**

*Creating an SMB share on a CIFS server* on page 177

*Adding or removing share properties on an existing SMB share* on page 183

**Enabling or disabling access-based enumeration from a Windows client**

You can enable or disable access-based enumeration (ABE) on SMB shares from a Windows client, which allows you to configure this share setting without needing to connect to the CIFS server.

**Step**

1. From a Windows client that supports ABE, enter the following command:

   ```
   abecmd [/enable | /disable] [/server CIFS_server_name] [/all | share_name]
   ```

   For more information about the `abecmd` command, see your Windows client documentation.
Configuring Data ONTAP for Microsoft Hyper-V and SQL Server over SMB solutions

With the new capabilities provided in Data ONTAP 8.2 and later, you can now use continuously available SMB 3.0 file shares to store Hyper-V virtual machine files or SQL Server system databases and user databases on volumes residing in Storage Virtual Machines (SVMs) with FlexVol volumes, while at the same time providing nondisruptive operations (NDOs) for both planned and unplanned events.

**Microsoft Hyper-V over SMB**

To create a Hyper-V over SMB solution, you must first configure Data ONTAP to provide storage services for Microsoft Hyper-V servers. Additionally, you must also configure Microsoft clusters (if using a clustered configuration), Hyper-V servers, continuously available SMB 3.0 connections to the shares hosted by the CIFS server, and, optionally, backup services to protect the virtual machine files that are stored on SVM volumes.

*Note:* The Hyper-V servers must be configured on Windows 2012 Server or later. Both stand-alone and clustered Hyper-V server configurations are supported.

- For information about creating Microsoft clusters and Hyper-V servers, see the Microsoft web site.
- SnapManager for Hyper-V is a host-based application that facilitates rapid, Snapshot copy-based backup services, designed to integrate with Hyper-V over SMB configurations.
  For information about using SnapManager with Hyper-V over SMB configurations, see SnapManager for Hyper-V Installation and Administration Guide.

**Microsoft SQL Server over SMB**

To create a SQL Server over SMB solution, you must first configure Data ONTAP to provide storage services for the Microsoft SQL Server application. Additionally, you must also configure Microsoft clusters (if using a clustered configuration). You would then install and configure SQL Server 2012 on the Windows servers and create continuously available SMB 3.0 connections to the shares hosted by the CIFS server. You can optionally configure backup services to protect the database files that are stored on SVM volumes.

*Note:* SQL Server must be installed and configured on Windows 2012 Server or later. Both stand-alone and clustered configurations are supported.

- For information about creating Microsoft clusters and installing and configuring SQL Server 2012, see the Microsoft web site.
- SnapManager for Microsoft SQL Server is a host-based application that facilitates rapid, Snapshot copy-based backup services, designed to integrate with SQL Server over SMB configurations.
  For information about using SnapManager for Microsoft SQL Server, see the SnapManager for Microsoft SQL Server Installation and Administration Guide.

**What nondisruptive operations for Hyper-V and SQL Server over SMB means**

Nondisruptive operations for Hyper-V and SQL Server over SMB refers to the combination of capabilities that enable the application servers and the contained virtual machines or databases to
remain online and to provide continuous availability during many administrative tasks. This includes both planned and unplanned downtime of the storage infrastructure.

Supported nondisruptive operations for application servers over SMB include the following:

- Planned takeover and giveback
- Unplanned takeover
- Upgrade
  To perform a nondisruptive upgrade (NDU), all nodes in the cluster must be running a version of clustered Data ONTAP that supports this functionality.
    - Data ONTAP 8.2 is the first release that supports NDUs for Hyper-V over SMB solutions; therefore, nondisruptive upgrades are supported if all nodes in the cluster are running Data ONTAP 8.2 or later, including upgrades within the Data ONTAP 8.2 release family.
    - Data ONTAP 8.2.1 is the first release that supports NDUs for SQL Server over SMB solutions; therefore, nondisruptive upgrades are supported if all nodes in the cluster are running Data ONTAP 8.2.1 or later, including upgrades within the Data ONTAP 8.2 release family to releases later than Data ONTAP 8.2.1.
- Planned aggregate relocation (ARL)
- LIF migration and failover
- Planned volume move

**Related concepts**

- *Key concepts about nondisruptive operations for Hyper-V and SQL Server over SMB* on page 374
- *Remote VSS concepts* on page 378

**Protocols that enable nondisruptive operations over SMB**

Along with the release of SMB 3.0, Microsoft has released new protocols to provide the capabilities necessary to support nondisruptive operations for Hyper-V and SQL Server over SMB.

Data ONTAP uses these protocols when providing nondisruptive operations for application servers over SMB:

- SMB 3.0
- Witness

**Related concepts**

- *How SMB 3.0 functionality supports nondisruptive operations over SMB shares* on page 376
- *What the Witness protocol does to enhance transparent failover* on page 376

**Key concepts about nondisruptive operations for Hyper-V and SQL Server over SMB**

There are certain concepts about nondisruptive operations (NDOs) that you should understand before you configure your Hyper-V or SQL Server over SMB solution.

**Continuously available share**

An SMB 3.0 share that has the continuously available share property set. Clients connecting through continuously available shares can survive disruptive events such as takeover, giveback, and aggregate relocation.

**Node**
A single controller that is a member of a cluster. To distinguish between the two nodes in an SFO pair, one node is sometimes called the local node and the other node is sometimes called the partner node or remote node. The primary owner of the storage is the local node. The secondary owner, which takes control of the storage when the primary owner fails, is the partner node. Each node is the primary owner of its storage and secondary owner for its partner's storage.

**Nondisruptive aggregate relocation**
The ability to move an aggregate between partner nodes within an SFO pair in a cluster without interrupting client applications.

**Nondisruptive failover**
See Takeover.

**Nondisruptive LIF migration**
The ability to perform a LIF migration without interrupting client applications that are connected to the cluster through that LIF. For SMB connections, this is only possible for clients that connect using SMB 2.0 or later.

**Nondisruptive operations**
The ability to perform major clustered Data ONTAP management and upgrade operations as well as withstand node failures without interrupting client applications. This term refers to the collection of nondisruptive takeover, nondisruptive upgrade, and nondisruptive migration capabilities as a whole.

**Nondisruptive upgrade**
The ability to upgrade node hardware or software without application interruption.

**Nondisruptive volume move**
The ability to move a volume freely throughout the cluster without interrupting any applications that are using the volume. For SMB connections, all versions of SMB support nondisruptive volume moves.

**Persistent handles**
A property of SMB 3.0 that allows continuously available connections to transparently reconnect to the CIFS server in the event of a disconnection. Similar to durable handles, persistent handles are maintained by the CIFS server for a period of time after communication to the connecting client is lost. However, persistent handles have more resilience than durable handles. In addition to giving the client a chance to reclaim the handle within a 60-second window after reconnecting, the CIFS server denies access to any other clients requesting access to the file during that 60-second window.

Information about persistent handles is mirrored on the SFO partner's persistent storage, which allows clients with disconnected persistent handles to reclaim the durable handles after an event where the SFO partner takes ownership of the node's storage. In addition to providing nondisruptive operations in the event of LIF moves (which durable handles support), persistent handles provide nondisruptive operations for takeover, giveback, and aggregate relocation.

**SFO giveback**
Returning aggregates to their home locations when recovering from a takeover event.

**SFO pair**
A pair of nodes whose controllers are configured to serve data for each other if one of the two nodes stops functioning. Depending on the system model, both controllers can be in a single chassis, or the controllers can be in separate chassis. Known as an HA pair in a two-node cluster.

**Takeover**
The process by which the partner takes control of the storage when the primary owner of that storage fails. In the context of SFO, failover and takeover are synonymous.

Related concepts

- Remote VSS concepts on page 378
- What the Witness protocol does to enhance transparent failover on page 376

How SMB 3.0 functionality supports nondisruptive operations over SMB shares

SMB 3.0 provides crucial functionality that enables support for nondisruptive operations for Hyper-V and SQL Server over SMB shares. This includes the new continuously-available share property and a new type of file handle known as a persistent handle that allow SMB clients to reclaim file open state and transparently reestablish SMB connections.

Persistent handles can be granted to SMB 3.0 capable clients that connect to a share with the continuously available share property set. If the SMB session is disconnected, the CIFS server retains information about persistent handle state. The CIFS server blocks other client requests during the 60-second period in which the client is allowed to reconnect, thus allowing the client with the persistent handle to reclaim the handle after a network disconnection. Clients with persistent handles can reconnect by using one of the data LIFs on the Storage Virtual Machine (SVM), either by reconnecting through the same LIF or through a different LIF.

Aggregate relocation, takeover, and giveback all occur between SFO pairs. To seamlessly manage the disconnection and reconnection of sessions with files that have persistent handles, the partner node maintains a copy of all persistent handle lock information. Whether the event is planned or unplanned, the SFO partner can nondisruptively manage the persistent handle reconnects. With this new functionality, SMB 3.0 connections to the CIFS server can transparently and nondisruptively fail over to another data LIF assigned to the SVM in what traditionally has been disruptive events.

Although the use of persistent handles allows the CIFS server to transparently fail over SMB 3.0 connections, if a failure causes the Hyper-V application to fail over to another node in the Windows Server 2012 cluster, the client has no way to reclaim the file handles of these disconnected handles. In this scenario, file handles in the disconnected state can potentially block access of the Hyper-V application if it is restarted on a different node. “Failover Clustering” is a part of SMB 3.0 that addresses this scenario by providing a mechanism to invalidate stale, conflicting handles. Using this mechanism, a Hyper-V cluster can recover quickly when Hyper-V cluster nodes fail.

Related concepts

- Supported SMB 3.0 functionality on page 105

Related tasks

- Creating Data ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server over SMB on page 393
- Enabling or disabling SMB 3.0 on page 107
- Configuring existing shares for continuous availability on page 403

What the Witness protocol does to enhance transparent failover

The Witness protocol provides enhanced client failover capabilities for SMB 3.0 continuously available shares (CA shares). Witness facilitates faster failover because it bypass the LIF failover
recovery period. It notifies applications servers when a node is unavailable without needing to wait for the SMB 3.0 connection to time out.

The failover is seamless, with applications running on the client not being aware that a failover occurred. If Witness is not available, failover operations still occur successfully, but failover without Witness is less efficient.

Witness enhanced failover is possible when the following requirements are met:

- It can only be used with SMB 3.0-capable CIFS servers that have SMB 3.0 enabled.
- The shares must use SMB 3.0 with the continuous availability share property set.
- The SFO partner of the node to which the application servers are connected must have at least one operational data LIF assigned to the Storage Virtual Machine (SVM) hosting data for the application servers.

  **Note:** The Witness protocol operates between SFO pairs. Because LIFs can migrate to any node within the cluster, any node might need to be the witness for its SFO partner.

  The Witness protocol cannot provide rapid failover of SMB connections on a given node if the SVM hosting data for the application servers does not have an active data LIF on the partner node. Therefore, every node in the cluster must have at least one data LIF for each SVM hosting one of these configurations.

- The application servers must connect to the CIFS server by using the CIFS server name that is stored in DNS instead of by using individual LIF IP addresses.

**Related tasks**

- *Creating Data ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server over SMB* on page 393
- *Verifying LIF status* on page 413

**How the Witness protocol works**

Data ONTAP implements the Witness protocol by using a node’s SFO partner as the witness. In the event of a failure, the partner quickly detects the failure and notifies the SMB client.

The Witness protocol provides enhanced failover using the following process:

1. When the application server establishes a continuously available SMB connection to Node1, the CIFS server informs the application server that Witness is available.
2. The application server requests the IP addresses of the Witness server from Node1 and receives a list of Node2 (the SFO partner) data LIF IP addresses assigned to the Storage Virtual Machine (SVM).
3. The application server chooses one of the IP addresses, creates a Witness connection to Node2, and registers to be notified if the continuously available connection on Node1 must move.
4. If a failover event occurs on Node1, Witness facilitates failover events, but is not involved with giveback.
5. Witness detects the failover event and notifies the application server through the Witness connection that the SMB connection must move to Node2.
6. The application server moves the SMB session to Node2 and recovers the connection without interruption to client access.
Share-based backups with Remote VSS

You can use Remote VSS to perform share-based backups of Hyper-V virtual machine files that are stored on a CIFS server.

Microsoft Remote VSS (Volume Shadow Copy Services) is an extension of the existing Microsoft VSS infrastructure. Previously, VSS could be used for backup services only for data stored on local disk. This limited the use of VSS to applications that store data either on a local disk or on SAN-based storage. With Remote VSS, Microsoft has extended the VSS infrastructure to support the shadow copying of SMB shares. Server applications such as Hyper-V are now storing VHD files on SMB file shares. With these new extensions, it is possible to take application consistent shadow copies for virtual machines that store data and configuration files on shares.

Related tasks

Creating Data ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server over SMB on page 393

Enabling or disabling VSS shadow copies for Hyper-V over SMB backups on page 405

Remote VSS concepts

You should be aware of certain concepts that are required to understand how Remote VSS (Volume Shadow Copy Service) is used by backup services with Hyper-V over SMB configurations.

VSS (Volume Shadow Copy Service)

A Microsoft technology that is used to take backup copies or snapshots of data on a specific volume at a specific point in time. VSS coordinates among data servers, backup applications, and storage management software to support the creation and management of consistent backups.

Remote VSS (Remote Volume Shadow Copy Service)

A Microsoft technology that is used to take share-based backup copies of data that is in a data-consistent state at a specific point in time where the data is accessed over SMB 3.0 shares. Also known as Volume Shadow Copy Service.

Shadow copy
A duplicate set of data contained in the share at a well-defined instant in time. Shadow copies are used to create consistent point-in-time backups of data, allowing the system or applications to continue updating data on the original volumes.

**Shadow copy set**
A collection of one or more shadow copies, with each shadow copy corresponding to one share. The shadow copies within a shadow copy set represent all the shares that must be backed up in the same operation. The VSS client on the VSS-enabled application identifies which shadow copies to include in the set.

**Shadow copy set automatic recovery**
The part of the backup process for remote VSS-enabled backup applications where the replica directory containing the shadow copies is made point-in-time consistent. At the start of the backup, the VSS client on the application triggers the application to take software checkpoints on the data scheduled for backup (the virtual machine files in the case of Hyper-V). The VSS client then allows the applications to continue. After the shadow copy set is created, Remote VSS makes the shadow copy set writable and exposes the writable copy to the applications. The application prepares the shadow copy set for backup by performing an automatic recovery using the software checkpoint taken earlier. Automatic recovery brings the shadow copies into a consistent state by unrolling the changes made to the files and directories since the checkpoint was created. Automatic recovery is an optional step for VSS-enabled backups.

**Shadow copy ID**
A GUID that uniquely identifies a shadow copy.

**Shadow copy set ID**
A GUID that uniquely identifies a collection of shadow copy IDs to the same server.

**SnapManager for Hyper-V**
The software that automates and simplifies backup-and-restore operations for Microsoft Windows Server 2012 Hyper-V. SnapManager for Hyper-V uses Remote VSS with automatic recovery to back up Hyper-V files over SMB shares.

**Related concepts**
- [Key concepts about nondisruptive operations for Hyper-V and SQL Server over SMB](#)
on page 374
- [Share-based backups with Remote VSS](#) on page 378

**Example of a directory structure used by Remote VSS**
Remote VSS traverses the directory structure on the that stores Hyper-V virtual machine files as it creates shadow copies. It is important to understand what an appropriate directory structure is so that backups of virtual machine files succeed.

A supported directory structure for successful shadow copy creation conforms to the following requirements:

- Only directories and regular files are present within the directory structure used to store virtual machine files.
  The directory structure does not contain junctions, links, or non-regular files.

- All files for a virtual machine reside within a single share.

- The directory structure used to store virtual machine files does not exceed the configured shadow copy directory depth.

- The root directory of the share contains only virtual machine files or directories.

In the following example, the volume named vm_vol1 is created with a junction point at `/hyperv/vm1` on Storage Virtual Machine (SVM) vs1. Subdirectories to contain the virtual machine
files are created under the junction point. The Hyper-V server's virtual machine files are accessed over share1 that has the path /hyperv/vm1/dir1/vmdir. The shadow copy service creates shadow copies of all the virtual machine files contained within the directory structure under share1 (up to the configured shadow copy directory depth).

How SnapManager for Hyper-V manages Remote VSS-based backups for Hyper-V over SMB

You can use SnapManager for Hyper-V to manage Remote VSS-based backup services. There are benefits to using SnapManager for Hyper-V managed backup service to create space efficient backup sets.

Optimizations to SnapManager for Hyper-V managed backups include the following:

- SnapDrive integration with Data ONTAP provides performance optimization when discovering SMB share location.
  Data ONTAP provides SnapDrive with the name of the volume where the share resides.

- SnapManager for Hyper-V specifies the list of virtual machine files in the SMB shares that the shadow copy service needs to copy.
  By providing a targeted list of virtual machine files, the shadow copy service does not need to creates shadow copies of all the files in the share.

- The Storage Virtual Machine (SVM) retains the Snapshot copies for SnapManager for Hyper-V to use for restores.
  There is no backup phase. The backup is the space-efficient Snapshot copy.

SnapManager for Hyper-V provides backup and restore capabilities for HyperV over SMB using the following process:

1. Preparing for the shadow copy operation
   The SnapManager for Hyper-V application's VSS client sets up the shadow copy set. The VSS client gathers information about what shares to include in the shadow copy set and provides this
information to Data ONTAP. A set might contain one or more shadow copies, and one shadow copy corresponds to one share.

2. Creating the shadow copy set (if automatic-recovery is used)
   For every share included in the shadow copy set, Data ONTAP creates a shadow copy and makes the shadow copy writable.

3. Exposing the shadow copy set
   After Data ONTAP creates the shadow copies, they are exposed to SnapManager for Hyper-V so that the application's VSS writers can perform automatic recovery.

4. Automatically recovering the shadow copy set
   During the shadow copy set creation, there is a period of time when active changes are occurring to the files included in the backup set. The application's VSS writers must update the shadow copies to make sure that they are in a completely consistent state prior to backup.
   
   Note: The way that automatic recovery is done is application specific. Remote VSS is not involved in this phase.

5. Completing and cleaning up the shadow copy set
   The VSS client notifies Data ONTAP after it completes automatic recovery. The shadow copy set is made read-only and then is ready for backup. When using SnapManager for Hyper-V for backup, the files in a Snapshot copy become the backup; therefore, for the backup phase, a Snapshot copy is created for every volume containing shares in the backup set. After the backup is complete, the shadow copy set is removed from the CIFS server.

How ODX copy offload is used with Hyper-V and SQL Server over SMB shares

Offloaded Data Transfer (ODX), also known as copy offload, enables direct data transfers within or between compatible storage devices without transferring the data through the host computer. Data ONTAP ODX copy offload provides you with performance benefits when performing copy operations on your application server over SMB installation.

In non-ODX file transfers, the data is read from the source CIFS server and is transferred across the network to the client computer. The client computer transfers the data back over the network to the destination CIFS server. In summary, the client computer reads the data from the source and writes it to the destination. With ODX file transfers, data is copied directly from the source to the destination.

Because ODX offloaded copies are performed directly between the source and destination storage, there are significant performance benefits. The performance benefits realized include faster copy time between source and destination, reduced resource utilization (CPU, memory) on the client, and reduced network I/O bandwidth utilization.

This functionality is available on Windows Server 2012 servers. Data ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0 continuously available connections.

The following use cases support using ODX copies and moves:

- **Intra-volume**
  The source and destination files or LUNs are within the same volume.

- **Inter-volume, same node, same Storage Virtual Machine (SVM)**
  The source and destination files or LUNs are on different volumes that are located on the same node. The data is owned by the same SVM.

- **Inter-volume, different nodes, same SVM**
  The source and destination files or LUNs are on different volumes that are located on different nodes. The data is owned by the same SVM.
• Inter-SVM, same node
  The source and destination file or LUNs are on different volumes that are located on the same
  node. The data is owned by different SVMs.

• Inter-SVM, different nodes
  The source and destination file or LUNs are on different volumes that are located on different
  nodes. The data is owned by different SVMs.

Specific use cases for ODX copy offload with Hyper-V solutions include the following:

• You can use ODX copy offload pass-through with Hyper-V to copy data within or across virtual
  hard disk (VHD) files or to copy data between mapped SMB shares and connected iSCSI LUNs
  within the same cluster.
  This allows copies from guest operating systems to pass through to the underlying storage.

• When creating fixed-sized VHDs, ODX is used for initializing the disk with zeros, using a well-
  known zeroed token.

• ODX copy offload is used for virtual machine storage migration if the source and destination
  storage is on the same cluster.

  Note: To take advantage of the use cases for ODX copy offload pass-through with Hyper-V, the
  guest operating system must support ODX and the guest operating system’s disks must be SCSI
  disks backed by storage (either SMB or SAN) that supports ODX. IDE disks on the guest
  operating system do not support ODX pass-through.

Specific use cases for ODX copy offload with SQL Server solutions include the following:

• You can use ODX copy offload to export and import SQL Server databases between mapped
  SMB shares or between SMB shares and connected iSCSI LUNs within the same cluster.

• ODX copy offload is used for database exports and imports if the source and destination storage
  is on the same cluster.

Related concepts
  
  Improving Microsoft remote copy performance on page 359

Related tasks
  
  Creating Data ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server
  over SMB on page 393

Configuration requirements and considerations

There are certain requirements and considerations that you must consider while planning and
configuring SQL Server and Hyper-V application servers for NDOs over SMB shares.

Related concepts
  
  Planning the Hyper-V or SQL Server over SMB configuration on page 390
  Considerations for reverting Hyper-V over SMB configurations on page 406

Related tasks
  
  Creating Data ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server
  over SMB on page 393
Data ONTAP and licensing requirements

You need to be aware of certain Data ONTAP and licensing requirements when creating SQL Server or Hyper-V over SMB solutions for nondisruptive operations on SVMs with FlexVol volumes. Hyper-V and SQL Server over SMB solutions are not supported on SVMs with Infinite Volume.

Data ONTAP version requirements

- **Hyper-V over SMB**
  Clustered Data ONTAP 8.2 and later releases support nondisruptive operations over SMB shares for Hyper-V running on Windows 2012 or later.

- **SQL Server over SMB**
  Clustered Data ONTAP 8.2.1 and later releases in the 8.2 release family support nondisruptive operations over SMB shares for SQL Server 2012 or later running on Windows 2012 or later.

For the latest information about supported versions of Data ONTAP, Windows Server, and SQL Server for nondisruptive operations over SMB shares, see the Interoperability Matrix at mysupport.netapp.com/matrix.

Licensing requirements

The following licenses are required:

- CIFS
- FlexClone (for Hyper-V over SMB only)
  This license is required if Remote VSS is used for backups. The shadow copy service uses FlexClone to create point-in-time copies of files that are then used when creating a backup. A FlexClone license is optional if you use a backup method that does not use Remote VSS.

Network and data LIF requirements

You need to be aware of certain network and data LIF requirements when creating SQL Server or Hyper-V over SMB configurations for nondisruptive operations.

Network protocol requirements

- IPv4 and IPv6 networks are supported.
- SMB 3.0 or later is required.
  SMB 3.0 provides the functionality needed to create the continuously available SMB connections necessary to offer nondisruptive operations.
- DNS servers must contain entries that map the CIFS server name to the IP addresses assigned to the data LIFs on the Storage Virtual Machine (SVM).
  The Hyper-V or SQL Server application servers typically make multiple connections over multiple data LIFs when accessing virtual machine or database files. For proper functionality, the application servers must make these multiple SMB connections by using the CIFS server name instead of making multiple connections to multiple unique IP addresses.
  Witness also requires the use of the CIFS server's DNS name instead of individual LIF IP addresses.

Data LIF requirements

- The SVM hosting the application server over SMB solution must have at least one operational data LIF on every node in the cluster.
SVM data LIFs can fail over to other data ports within the cluster, including nodes that are not currently hosting data accessed by the application servers. Additionally, because the Witness node is always the SFO partner of a node to which the application server is connected, every node in the cluster is a potential Witness node.

- Data LIFs must not be configured to automatically revert. After a takeover or giveback event, you should manually revert the data LIFs to their home ports.
- All data LIF IP addresses must have an entry in DNS and all entries must resolve to the CIFS server name. The application servers must connect to SMB shares by using the CIFS server name. You must not configure the application servers to make connections by using the LIF IP addresses.
- If the CIFS server name is different from the SVM name, the DNS entries must resolve to the CIFS server name.

**CIFS server and volume requirements for Hyper-V over SMB**

You need to be aware of certain CIFS server and volume requirements when creating Hyper-V over SMB configurations for nondisruptive operations.

**CIFS server requirements**

- SMB 3.0 must be enabled. This is enabled by default.
- The default UNIX user CIFS server option must be configured with a valid UNIX user account. The application servers use the machine account when creating an SMB connection. Because all SMB access requires that the Windows user successfully map to a UNIX user account or to the default UNIX user account, Data ONTAP must be able to map the application server’s machine account to the default UNIX user account.
- Automatic node referrals must be disabled. Automatic node referrals are disabled by default. If you want to use automatic node referrals for access to data other than Hyper-V machine files, you must create a separate SVM for that data.
- Both Kerberos and NTLM authentication must be allowed in the domain to which the CIFS server belongs. Data ONTAP does not advertise the Kerberos service for Remote VSS; therefore, the domain should be set to permit NTLM.
- Shadow copy functionality must be enabled. This functionality is enabled by default.
- The Windows domain account that the shadow copy service uses when creating shadow copies must be a member of the CIFS server's local BUILTIN\Administrators or BUILTIN\Backup Operators group.

**Volume requirements**

- Volumes used to store virtual machine files must be created as NTFS security-style volumes. To provide NDOs for application servers using continuously available SMB connections, the volume containing the share must be an NTFS volume. Moreover, it must always have been an NTFS volume. You cannot change a mixed security-style volume or UNIX security-style volume to an NTFS security-style volume and directly use it for NDOs over SMB shares. If you change a mixed security-style volume to an NTFS security style volume and intend to use it for NDOs over SMB shares, you must manually place an ACL at the top of the volume and propagate that ACL to all contained files and folders. Otherwise, virtual machine migrations or database file exports and imports where files are moved to another volume can fail if either the source or the
destination volumes were initially created as mixed or UNIX security-style volumes and later changed to NTFS security style.

- For shadow copy operations to succeed, you must have enough available space on the volume. The available space must be at least as large as the combined space used by all files, directories, and subdirectories contained within the shares included in the shadow copy backup set. This requirement only applies to shadow copies with auto-recovery.

Related information


CIFS server and volume requirements for SQL Server over SMB

You need to be aware of certain CIFS server and volume requirements when creating SQL Server over SMB configurations for nondisruptive operations.

CIFS server requirements

- SMB 3.0 must be enabled.
  This is enabled by default.

- The default UNIX user CIFS server option must be configured with a valid UNIX user account.
  The application servers use the machine account when creating an SMB connection. Because all SMB access requires that the Windows user successfully map to a UNIX user account or to the default UNIX user account, Data ONTAP must be able to map the application server's machine account to the default UNIX user account.
  Additionally, SQL Server uses a domain user as the SQL Server service account. The service account must also map to the default UNIX user.

- Automatic node referrals must be disabled.
  Automatic node referrals are disabled by default. If you want to use automatic node referrals for access to data other than SQL server database files, you must create a separate SVM for that data.

- The Windows user account used for installing SQL Server on Data ONTAP must be assigned the SeSecurityPrivilege privilege.
  This privilege is assigned to the CIFS server's local BUILTIN\Administrators group.

Volume requirements

- Volumes used to store virtual machine files must be created as NTFS security-style volumes.
  To provide NDOs for application servers using continuously available SMB connections, the volume containing the share must be an NTFS volume. Moreover, it must always have been an NTFS volume. You cannot change a mixed security-style volume or UNIX security-style volume to an NTFS security-style volume and directly use it for NDOs over SMB shares. If you change a mixed security-style volume to an NTFS security style volume and intend to use it for NDOs over SMB shares, you must manually place an ACL at the top of the volume and propagate that ACL to all contained files and folders. Otherwise, virtual machine migrations or database file exports and imports where files are moved to another volume can fail if either the source or the destination volumes were initially created as mixed or UNIX security-style volumes and later changed to NTFS security style.

- Although the volume containing the database files can contain junctions, SQL Server does not cross junctions when creating the database directory structure.

- For SnapManager for Microsoft SQL Server backup operations to succeed, you must have enough available space on the volume.
  The volume on which the SQL Server database files reside must be large enough to hold the database directory structure and all contained files residing within the share.
Continuously available share requirements and considerations for Hyper-V over SMB

You need to be aware of certain requirements and considerations when configuring continuously available shares for Hyper-V over SMB configurations that support nondisruptive operations.

Share requirements

- Shares used by the application servers must be configured with the continuously available property set.
  Application servers that connect to continuously available shares receive persistent handles that allow them to reconnect nondisruptively to SMB shares and reclaim file locks after disruptive events such as takeover, giveback, and aggregate relocation.

- If you want to use Remote VSS-enabled backup services, you cannot put Hyper-V files into shares that contain junctions.
  In the auto-recovery case, the shadow copy creation fails if a junction is encountered while traversing the share. In the non auto-recovery case, the shadow copy creation does not fail, but the junction does not point to anything.

- If you want to use Remote VSS-enabled backup services with auto-recovery, you cannot put Hyper-V files into shares that contain the following:
  - Symlinks, hardlinks, or widelinks
  - Non-regular files
    The shadow copy creation fails if there are any links or non-regular files in the share to shadow copy. This requirement only applies to shadow copies with auto-recovery.
  - For shadow copy operations to succeed, you must have enough available space on the volume (for Hyper-V over SMB only).
    The available space must be at least as large as the combined space used by all files, directories, and subdirectories contained within the shares included in the shadow copy backup set. This requirement only applies to shadow copies with auto-recovery.

- The following share properties must not be set on continuously available shares used by the application servers:
  - Home directory
  - Change notify
  - Attribute caching
  - BranchCache
  - Access-based enumerations

  **Note:** With change notify disabled, Windows 2012 Server does not refresh the Explorer window, which causes an inconsistent view of directory contents.

Considerations

- Quotas are not supported on continuously available shares.
  Even if a quota is specified, the continuously available share ignores quota policies.

- The following functionality is not supported for Hyper-V over SMB configurations:
Auditing
FPolicy

- Virus scanning is not performed on SMB shares with the `continuously-availability` parameter set to **Yes**.

**Continuously available share requirements and considerations for SQL Server over SMB**

You need to be aware of certain requirements and considerations when configuring continuously available shares for SQL Server over SMB configurations that support nondisruptive operations.

**Share requirements**

- Volumes used to store virtual machine files must be created as NTFS security-style volumes.
  To provide nondisruptive operations for application servers using continuously available SMB connections, the volume containing the share must be an NTFS volume. Moreover, it must always have been an NTFS volume. You cannot change a mixed security-style volume or UNIX security-style volume to an NTFS security-style volume and directly use it for nondisruptive operations over SMB shares. If you change a mixed security-style volume to an NTFS security style volume and intend to use it for nondisruptive operations over SMB shares, you must manually place an ACL at the top of the volume and propagate that ACL to all contained files and folders. Otherwise, virtual machine migrations or database file exports and imports where files are moved to another volume can fail if either the source or the destination volumes were initially created as mixed or UNIX security-style volumes and later changed to NTFS security style.

- Shares used by the application servers must be configured with the continuously available property set.
  Application servers that connect to continuously available shares receive persistent handles that allow them to reconnect nondisruptively to SMB shares and reclaim file locks after disruptive events such as takeover, giveback, and aggregate relocation.

- Although the volume containing the database files can contain junctions, SQL Server does not cross junctions when creating the database directory structure.

- For SnapManager for Microsoft SQL Server backup operations to succeed, you must have enough available space on the volume.
  The volume on which the SQL Server database files reside must be large enough to hold the database directory structure and all contained files residing within the share.

- The following share properties must not be set on continuously available shares used by the application servers:
  - Home directory
  - Change notify
  - Attribute caching
  - BranchCache
  - Access-based enumerations

  **Note:** With change notify disabled, Windows 2012 Server does not refresh the Explorer window, which causes an inconsistent view of directory contents.

**Share considerations**

- Quotas are not supported on continuously available shares.
Even if a quota is specified, the continuously available share ignores quota policies.

- The following functionality is not supported for SQL Server over SMB configurations:
  - Auditing
  - FPolicy
- Virus scanning is not performed on SMB shares with the continuously-availability share property set.

**Remote VSS considerations for Hyper-V over SMB configurations**

You need to be aware of certain considerations when using Remote VSS-enabled backup solutions for Hyper-V over SMB configurations.

**General Remote VSS considerations**

- A maximum of 64 shares can be configured per Microsoft application server. The shadow copy operation fails if there are more than 64 shares in a shadow copy set. This is a Microsoft requirement.

- Only one active shadow copy set per CIFS server is allowed. A shadow copy operation will fail if there is an ongoing shadow copy operation on the same CIFS server. This is a Microsoft requirement.

- No junctions are allowed within the directory structure on which Remote VSS creates a shadow copy.
  - In the automatic recovery case, the shadow copy creation will fail if a junction is encountered while traversing the share.
  - In the nonautomatic recovery case, the shadow copy creation does not fail, but the junction does not point to anything.

**Remote VSS considerations that apply only for shadow copies with automatic recovery**

Certain limits apply only for shadow copies with automatic recovery.

- A maximum directory depth of five subdirectories is allowed for shadow copy creation. This is the directory depth over which the shadow copy service creates a shadow copy backup set. Shadow copy creation fails if directories containing virtual machine file are nested deeper than five levels. This is intended to limit the directory traversal when cloning the share. The maximum directory depth can be changed by using a CIFS server option.

- Amount of available space on the volume must be adequate. The available space must be at least as large as the combined space used by all files, directories, and subdirectories contained within the shares included in the shadow copy backup set.

- No links or non-regular files are allowed within the directory structure on which Remote VSS creates a shadow copy. The shadow copy creation fails if there are any links or non-regular files in the share to the shadow copy. The clone process does not support them.

- No NFSv4 ACLs are allowed on directories. Although shadow copy creation retains NFSv4 ACLs on files, the NFSv4 ACLs on directories are lost.

- A maximum of 60 seconds is allowed to create a shadow copy set.
Microsoft specifications allow a maximum of 60 seconds to create the shadow copy set. If the VSS client cannot create the shadow copy set within this time, the shadow copy operation fails; therefore, this limits the number of files in a shadow copy set. The actual number of files or virtual machines that can be included in a backup set varies; that number is dependent on many factors, and must be determined for each customer environment.

**ODX copy offload requirements for SQL Server and Hyper-V over SMB**

ODX copy offload must be enabled if you want to migrate virtual machine files or export and import database files directly from source to the destination storage location without sending data through the application servers. There are certain requirements that you must understand about using ODX copy offload with SQL Server and Hyper-V over SMB solutions.

Using ODX copy offload provides a significant performance benefit. This CIFS server option is enabled by default.

- SMB 3.0 must be enabled to use ODX copy offload.
- Source volumes must be a minimum of 1.25 GB.
- Deduplication must be enabled on volumes used with copy offload.
- Compression must not be enabled on volumes used with copy offload.
- To use ODX copy offload to migrate Hyper-V guests within and between disks, the Hyper-V servers must be configured to use SCSI disks.
  The default is to configure IDE disks, but ODX copy offload does not work when guests are migrated if disks are created using IDE disks.

**Recommendations for SQL Server and Hyper-V over SMB configurations**

To ensure that your SQL Server and Hyper-V over SMB configurations are robust and operational, you need to be familiar with recommended best practices when configuring the solutions.

**General recommendations**

- Separate application server files from general user data.
  If possible, devote an entire Storage Virtual Machine (SVM) and its storage for the application server's data.
- For best performance, do not enable SMB signing on SVMs that are used to store the application server's data.
- Do not create continuously available shares on any shares other than those used in the Hyper-V or SQL Server over SMB configuration.
- Disable change notify on shares used for continuous availability.
- Do not perform a volume move at the same time as ARL because ARL has phases that pause some operations.
- For Hyper-V over SMB solutions, use iSCSI drives when creating virtual machines or when adding disks to an existing virtual machine.
Planning the Hyper-V or SQL Server over SMB configuration

Before you configure Hyper-V or SQL Server over SMB for nondisruptive operations, you must understand the choices you need to make when creating the configuration. This can help you create a configuration that follows the best practices and recommendations.

Related concepts

Configuration requirements and considerations on page 382

Related tasks

Creating Data ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server over SMB on page 393

Completing the volume configuration worksheet

The worksheet provides an easy way to record the values that you need when creating volumes for SQL Server and Hyper-V over SMB configurations.

For each volume, you must specify the following information:

- Storage Virtual Machine (SVM) name
  The SVM name is the same for all volumes.
- Volume name
- Aggregate name
  You can create volumes on aggregates located on any node in the cluster.
- Size
- Junction path

You should keep the following in mind when creating volumes used to store application server data:

- If the root volume does not have NTFS security style, you must specify the security style as NTFS when you create the volume.
  By default, volumes inherit the security style of the SVM root volume.
- Volumes should be configured with the default volume space guarantee.
- You can optionally configure the autosize space management setting.
- You should set the option that determines the Snapshot copy space reserve to 0.
- The Snapshot policy applied to the volume must be disabled.
  If the SVM Snapshot policy is disabled, then you do not need to specify a Snapshot policy for the volumes. The volumes inherit the Snapshot policy for the SVM. If the Snapshot policy for the SVM is not disabled and is configured to create Snapshot copies, you must specify a Snapshot policy at the volume level, and that policy must be disabled. Shadow copy service-enabled backups and SQL Server backups manage Snapshot copy creation and deletion.
- You cannot configure load-sharing mirrors for the volumes.

Junction paths on which you plan to create shares that the application servers use should be chosen so that there are no junctioned volumes below the share entry point.

For example, if you want to store virtual machine files on four volumes named “vol1”, “vol2”, “vol3”, and “vol4”, you can create the namespace shown in the example. You can then create shares
for the application servers at the following paths: /data1/vol1, /data1/vol2, /data2/vol3, and /data2/vol4.

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Volume</th>
<th>Junction</th>
<th>Active</th>
<th>Junction Path</th>
<th>Path Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>data1</td>
<td></td>
<td>true</td>
<td>/data1</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>vol1</td>
<td></td>
<td>true</td>
<td>/data1/vol1</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>vol2</td>
<td></td>
<td>true</td>
<td>/data1/vol2</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>data2</td>
<td></td>
<td>true</td>
<td>/data2</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>vol3</td>
<td></td>
<td>true</td>
<td>/data2/vol3</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>vol4</td>
<td></td>
<td>true</td>
<td>/data2/vol4</td>
<td>RW_volume</td>
</tr>
</tbody>
</table>

**Types of information**

<table>
<thead>
<tr>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume 1: Volume name, aggregate, size, junction path</td>
</tr>
<tr>
<td>Volume 2: Volume name, aggregate, size, junction path</td>
</tr>
<tr>
<td>Volume 3: Volume name, aggregate, size, junction path</td>
</tr>
<tr>
<td>Volume 4: Volume name, aggregate, size, junction path</td>
</tr>
<tr>
<td>Volume 5: Volume name, aggregate, size, junction path</td>
</tr>
<tr>
<td>Volume 6: Volume name, aggregate, size, junction path</td>
</tr>
</tbody>
</table>

**Completing the SMB share configuration worksheet**

Use this worksheet to record the values that you need when creating continuously available SMB shares for SQL Server and Hyper-V over SMB configurations.

**Information about SMB shares properties and configuration settings**

For each share, you must specify the following information:

- Storage Virtual Machine (SVM) name
  - The SVM name is the same for all shares
- Share name
- Path
- Share properties
  - You must configure the following two share properties:
    - oplocks
    - continuously-available
  - The following share properties must not be set:
    - homedirectory
    - changenotify
• **attributecache**

• **branchcache**

• **access-based-enumeration**

  **Note:** With change notify disabled, Windows 2012 Server does not refresh the Explorer window, which causes an inconsistent view of directory contents.

• Symlinks must be disabled (the value for the `-symlink-properties` parameter must be null `""`).

**Information about share paths**

If you are using Remote VSS to back up Hyper-V files, the choice of share paths to use when making SMB connections from the Hyper-V servers to the storage locations where the virtual machine files are stored is important. Although shares can be created at any point in the namespace, paths for shares that the Hyper-V servers use should not contain junctioned volumes. Shadow copy operations cannot be performed on share paths that contain junction points.

SQL Server cannot cross junctions when creating the database directory structure. You should not create share paths for SQL server that contain junction points.

For example, given the namespace shown, if you want to store virtual machine files or database files on volumes “vol1”, “vol2”, “vol3”, and “vol4”, you should create shares for the application servers at the following paths: /data1/vol1, /data1/vol2, /data2/vol3, and /data2/vol4.

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Volume</th>
<th>Junction Active</th>
<th>Junction Path</th>
<th>Path Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>data1</td>
<td>true</td>
<td>/data1</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>vol1</td>
<td>true</td>
<td>/data1/vol1</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>vol2</td>
<td>true</td>
<td>/data1/vol2</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>data2</td>
<td>true</td>
<td>/data2</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>vol3</td>
<td>true</td>
<td>/data2/vol3</td>
<td>RW_volume</td>
</tr>
<tr>
<td>vs1</td>
<td>vol4</td>
<td>true</td>
<td>/data2/vol4</td>
<td>RW_volume</td>
</tr>
</tbody>
</table>

**Note:** Although you can create shares on the /data1 and /data2 paths for administrative management, you must not configure the application servers to use those shares to store data.

**Planning worksheet**

<table>
<thead>
<tr>
<th>Types of information</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume 1: SMB share name and path</td>
<td></td>
</tr>
<tr>
<td>Volume 2: SMB share name and path</td>
<td></td>
</tr>
<tr>
<td>Volume 3: SMB share name and path</td>
<td></td>
</tr>
<tr>
<td>Volume 4: SMB share name and path</td>
<td></td>
</tr>
<tr>
<td>Volume 5: SMB share name and path</td>
<td></td>
</tr>
<tr>
<td>Volume 6: SMB share name and path</td>
<td></td>
</tr>
<tr>
<td>Volume 7: SMB share name and path</td>
<td></td>
</tr>
<tr>
<td>Additional volumes: SMB share names and paths</td>
<td></td>
</tr>
</tbody>
</table>
Creating Data ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server over SMB

There are several Data ONTAP configuration steps you must perform to prepare for Hyper-V and SQL Server installations that provides nondisruptive operations over SMB.

Before you begin
Before you create the Data ONTAP configuration for nondisruptive operations with Hyper-V and SQL Server over SMB, the following tasks must be completed:

• Time services must be set up on the cluster.
• Networking must be set up for the SVM.
• The SVM must be created.
• Data LIF interfaces must be configured on the SVM.
• DNS must be configured on the SVM.
• Desired names services must be set up for the SVM.
• The CIFS server must be created.

Steps
1. Verifying that both Kerberos and NTLMv2 authentication are permitted (Hyper-V over SMB shares) on page 394
   Nondisruptive operations for Hyper-V over SMB require that the CIFS server on a data SVM and the Hyper-V server permit both Kerberos and NTLMv2 authentication. You must verify settings on both the CIFS server and the Hyper-V servers that control what authentication methods are permitted.

2. Verifying that domain accounts map to the default UNIX user on page 395
   Hyper-V and SQL Server use domain accounts to create SMB connections to continuously available shares. To successfully create the connection, the computer account must successfully map to a UNIX user. The most convenient way to accomplish this is to map the computer account to the default UNIX user.

3. Verifying that the security style of the SVM root volume is set to NTFS on page 397
   To ensure that nondisruptive operations for Hyper-V and SQL Server over SMB are successful, volumes must be created with NTFS security style. Since the root volume's security style is applied by default to volumes created on the Storage Virtual Machine (SVM), the security style of the root volume should be set to NTFS.

4. Verifying that required CIFS server options are configured on page 398
   You must verify that the required CIFS server options are enabled and configured according to requirements for nondisruptive operations for Hyper-V and SQL Server over SMB.

5. Verifying that automatic node referrals are disabled on page 399
   Automatic node referrals are not supported for nondisruptive operations with Hyper-V and SQL Server over SMB configurations. You must verify that automatic node referrals are disabled on CIFS servers that provide nondisruptive operations for application servers over SMB.

6. Creating NTFS data volumes on page 400
   You must create NTFS data volumes on the Storage Virtual Machine (SVM) before you can configure continuously available shares for use with Hyper-V or SQL Server over SMB application servers. Use the volume configuration worksheet to create your data volumes.
7. Creating continuously available SMB shares on page 401
   After you create your data volumes, you can create the continuously available shares that the
   application servers use to access Hyper-V virtual machine and configuration files and SQL Server
   database files. You should use the share configuration worksheet as you create the SMB shares.

8. Adding the SeSecurityPrivilege privilege to the user account (for SQL Server of SMB shares) on
   page 402
   The domain user account used for installing the SQL server must be assigned the
   “SeSecurityPrivilege” privilege to perform certain actions on the CIFS server that require
   privileges not assigned by default to domain users.

9. Configuring the VSS shadow copy directory depth (for Hyper-V over SMB shares) on page 402
   Optionally, you can configure the maximum depth of directories within SMB shares on which to
   create shadow copies. This parameter is useful if you want to manually control the maximum level
   of subdirectories on which Data ONTAP should create shadow copies.

Related concepts
   Planning the Hyper-V or SQL Server over SMB configuration on page 390
   Configuration requirements and considerations on page 382

Related tasks
   Setting the CIFS server minimum authentication security level on page 83

Verifying that both Kerberos and NTLMv2 authentication are permitted (Hyper-V over SMB shares)

Nondisruptive operations for Hyper-V over SMB require that the CIFS server on a data SVM and the
Hyper-V server permit both Kerberos and NTLMv2 authentication. You must verify settings on both
the CIFS server and the Hyper-V servers that control what authentication methods are permitted.

About this task
Kerberos authentication is required when making a continuously available share connection. Part of
the Remote VSS process uses NTLMv2 authentication. Therefore, connections using both
authentication methods must be supported for Hyper-V over SMB configurations.

The following settings must be configured to allow both Kerberos and NTLMv2 authentication:

- Export policies for SMB must be disabled on the Storage Virtual Machine (SVM).
  Both Kerberos and NTLMv2 authentication are always enabled on SVMs, but export policies can
  be used to restrict access based on authentication method.
  Prior to Data ONTAP 8.2, configuring export policies for SMB access was a requirement. Export
  policies control what types of authentication are allowed when accessing data using NAS
  protocols.
  Starting with Data ONTAP 8.2 and later releases, export policies for SMB are optional and are
  disabled by default. If export policies are disabled, both Kerberos and NTLMv2 authentication
  are allowed on a CIFS server by default.

- The domain to which the CIFS server and Hyper-V servers belong must permit both Kerberos and
  NTLMv2 authentication.
  Kerberos authentication is enabled by default on Active Directory domains. However, NTLMv2
  authentication can be disallowed, either using Security Policy settings or Group Policies.

Steps
   1. Perform the following to verify that export policies are disabled on the SVM:
      a. Set the privilege level to advanced:
set -privilege advanced

b. Verify that the -is-exportpolicy-enabled CIFS server option is set to false:

vserver cifs options show -vserver vserver_name -fields vserver,is-exportpolicy-enabled

c. Return to the admin privilege level:

set -privilege admin

2. If export policies for SMB are not disabled, disable them:

vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled false

3. Verify that both NTLMv2 and Kerberos authentication are allowed in the domain.

For information about determining what authentication methods are allowed in the domain, see the Microsoft TechNet Library.

4. If the domain does not permit NTLMv2 authentication, enable NTLMv2 authentication by using one of the methods described in Microsoft documentation.

Example

The following commands verify that export policies for SMB are disabled on SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only when directed to do so by technical support personnel. Do you wish to continue? (y or n): y
cluster1::*> vserver cifs options show -vserver vs1 -fields vserver,is-exportpolicy-enabled
vserver  is-exportpolicy-enabled
-------- -----------------------
vs1      false
cluster1::*> set -privilege admin
```

Verifying that domain accounts map to the default UNIX user

Hyper-V and SQL Server use domain accounts to create SMB connections to continuously available shares. To successfully create the connection, the computer account must successfully map to a UNIX user. The most convenient way to accomplish this is to map the computer account to the default UNIX user.

About this task

Hyper-V and SQL Server use the domain computer accounts to create SMB connections. In addition, SQL Server uses a domain user account as the service account that also makes SMB connections.

Starting with Data ONTAP 8.2 and later releases, when you create a Storage Virtual Machine (SVM), Data ONTAP automatically creates the default user named “pcuser” (with a UID of 65534) and the group named “pcuser” (with a GID of 65534), and adds the default user to the “pcuser” group. If you are configuring a Hyper-V over SMB solution on an SVM that existed prior to upgrading the cluster to Data ONTAP 8.2, the default user and group might not exist. If they do not, you must create them before configuring the CIFS server’s default UNIX user.

Steps

1. Determine whether there is a default UNIX user:
vserver cifs options show -vserver vserver_name

2. If the default user option is not set, determine whether there is a UNIX user that can be designated as the default UNIX user:

vserver services unix-user show -vserver vserver_name

3. If the default user option is not set and there is not a UNIX user that can be designated as the default UNIX user, create the default UNIX user and the default group, and add the default user to the group.

Generally, the default user is given the user name “pcuser” and must be assigned the UID of 65534. The default group is generally given the group name “pcuser”. The GID assigned to the group must be 65534.

a. Create the default group:

vserver services unix-group create -vserver vserver_name -name pcuser -id 65534

b. Create the default user and add the default user to the default group:

vserver services unix-user create -vserver vserver_name -user pcuser -id 65534 -primary-gid 65534

c. Verify that the default user and default group are configured correctly:

vserver services unix-user show -vserver vserver_name
vserver services unix-group show -vserver vserver_name -members

4. If the CIFS server's default user is not configured, perform the following:

a. Configure the default user:

vserver cifs options modify -vserver vserver_name -default-unix-user pcuser

b. Verify that the default UNIX user is configured correctly:

vserver cifs options show -vserver vserver_name

5. To verify that the application server's computer account correctly maps to the default user, map a drive to a share residing on the SVM and confirm the Windows user to UNIX user mapping by using the vserver cifs session show command.

For more information about using this command, see the man pages.

Example

The following commands determine that the CIFS server's default user is not set, but determines that the “pcuser” user and “pcuser” group exist. The “pcuser” user is assigned as the CIFS server's default user on SVM vs1.

cluster1::> vserver cifs options show
Vserver: vs1

Client Session Timeout : 900
Default Unix Group     : -
Default Unix User      : -
Guest Unix User        : -
Read Grants Exec       : disabled
Read Only Delete       : disabled
WINS Servers           : -

cluster1::> vserver services unix-user show

<table>
<thead>
<tr>
<th>User</th>
<th>User</th>
<th>Group</th>
<th>Full</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vserver Name</td>
<td>ID</td>
<td>ID</td>
<td>Name</td>
</tr>
</tbody>
</table>

For more information about using this command, see the man pages.
Verifying that the security style of the SVM root volume is set to NTFS

To ensure that nondisruptive operations for Hyper-V and SQL Server over SMB are successful, volumes must be created with NTFS security style. Since the root volume's security style is applied by default to volumes created on the Storage Virtual Machine (SVM), the security style of the root volume should be set to NTFS.

About this task

• You can specify the root volume security style at the time you create the SVM.

• If the SVM is not created with the root volume set to NTFS security style, you can change the security style later by using the `volume modify` command.

Steps

1. Determine the current security style of the SVM root volume:
   
   ```
   cluster1::> volume show -vserver vserver_name -fields vserver,volume,security-style
   ```

2. If the root volume is not an NTFS security-style volume, change the security style to NTFS:
   
   ```
   cluster1::> volume modify -vserver vserver_name -volume root_volume_name -security-style ntfs
   ```

3. Verify that the SVM root volume is set to NTFS security style:
   
   ```
   cluster1::> volume show -vserver vserver_name -fields vserver,volume,security-style
   ```

Example

The following commands verify that the root volume security style is NTFS on SVM vs1:

```
Verifying that required CIFS server options are configured

You must verify that the required CIFS server options are enabled and configured according to requirements for nondisruptive operations for Hyper-V and SQL Server over SMB.

About this task

- SMB 2.x and SMB 3.0 must be enabled.
- ODX copy offload must be enabled to use performance enhancing copy offload.
- VSS Shadow Copy services must be enabled if the Hyper-V over SMB solution uses Remote VSS-enabled backup services (Hyper-V only).

Steps

1. Verify that the required CIFS server options are enabled on the Storage Virtual Machine (SVM):
   a. Set the privilege level to advanced:
      ```
      set -privilege advanced
      ```
   b. Enter the following command:
      ```
      vserver cifs options show -vserver vserver_name
      ```
      The following options should be set to `true`:
      - `-smb2-enabled`
      - `-smb3-enabled`
      - `-copy-offload-enabled`
      - `-shadowcopy-enabled` (Hyper-V only)

2. If any of the options are not set to `true`, perform the following:
   a. Set them to `true` by using the `vserver cifs options modify` command.
   b. Verify that the options are set to `true` by using the `vserver cifs options show` command.

3. Return to the admin privilege level:
   ```
   set -privilege admin
   ```

Example

The following commands verify that the required options for the Hyper-V over SMB configuration are enabled on SVM vs1. In the example, ODX copy offload must be enabled to meet the option requirements.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y
```
Verifying that automatic node referrals are disabled

Automatic node referrals are not supported for nondisruptive operations with Hyper-V and SQL Server over SMB configurations. You must verify that automatic node referrals are disabled on CIFS servers that provide nondisruptive operations for application servers over SMB.

About this task

Automatic node referrals are disabled by default. If you have enabled them on the CIFS server that will provide nondisruptive services over SMB shares, you must disable them.

Steps

1. Perform the following to verify that automatic node referrals are disabled on the CIFS server:
   a. Set the privilege level to advanced:
      ```bash
      set -privilege advanced
      ```
   b. Verify that the `-is-referral-enabled` CIFS server option is set to `false`:
      ```bash
      vserver cifs options show -vserver vserver_name -fields is-referral-enabled
      ```

2. If automatic node referrals are not disabled, perform the following:
   a. Disable automatic node referrals:
      ```bash
      vserver cifs options modify -vserver vserver_name -is-referral-enabled false
      ```
   b. Verify that the new setting is correct:
      ```bash
      vserver cifs options show -vserver vserver_name -fields is-referral-enabled
      ```

3. Return to the admin privilege level:
   ```bash
   set -privilege admin
   ```

Example

The following commands verify that automatic node referrals are disabled on Storage Virtual Machine (SVM, formerly known as Vserver) vs1:

```bash
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y
cluster1::> vserver cifs options show -vserver vs1 -fields is-referral-enabled
```
Creating NTFS data volumes

You must create NTFS data volumes on the Storage Virtual Machine (SVM) before you can configure continuously available shares for use with Hyper-V or SQL Server over SMB application servers. Use the volume configuration worksheet to create your data volumes.

About this task

There are optional parameters that you can use to customize a data volume. For more information about customizing volumes, see the Clustered Data ONTAP Logical Storage Management Guide.

As you create your data volumes, you should not create junction points within a volume that contains the following:

- Hyper-V files for which Data ONTAP makes shadow copies
- SQL Server database files that are backed up using SQL Server

Note: If you inadvertently create a volume that uses mixed or UNIX security style, you cannot change the volume to an NTFS security style volume and then directly use it to create continuously available shares for nondisruptive operations. Nondisruptive operations for Hyper-V and SQL Server over SMB do not work correctly unless the volumes used in the configuration are created as NTFS security-style volumes.

You must either delete the volume and re-create the volume with NTFS security style, or you can map the volume on a Windows host and apply an ACL at the top of the volume and propagate the ACL to all files and folders in the volume.

Steps

1. Create the data volume by entering the appropriate command:

<table>
<thead>
<tr>
<th>If you want to create a volume in an SVM where the root volume security style is...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTFS</td>
<td>`volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size integer[KB</td>
</tr>
<tr>
<td>Not NTFS</td>
<td>`volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size integer[KB</td>
</tr>
</tbody>
</table>

2. Verify that the volume configuration is correct:

   `volume show -vserver vserver_name -volume volume_name`
Creating continuously available SMB shares

After you create your data volumes, you can create the continuously available shares that the application servers use to access Hyper-V virtual machine and configuration files and SQL Server database files. You should use the share configuration worksheet as you create the SMB shares.

Steps
1. Display information about the existing data volumes and their junction paths:
   ```
   volume show -vserver vserver_name -junction
   ```
2. Create a continuously available SMB share by entering the following command:
   ```
   vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties oplocks,continuously-available -symlink "" [-comment text]
   ```
   - You can optionally add a comment to the share configuration.
   - By default, the offline files share property is configured on the share and is set to manual.
   - Data ONTAP creates the share with the Windows default share permission of Everyone/Full Control.
3. Repeat the previous step for all shares in the share configuration worksheet.
4. Verify that your configuration is correct by using the `vserver cifs share show` command.
5. Configure NTFS file permissions on the continuously available shares by mapping a drive to each share, and configuring file permissions by using the Windows Properties window.

Example

The following commands create a continuously available share named “data2” on Storage Virtual Machine (SVM, formerly known as Vserver) vs1. Symlinks are disabled by setting the -symlink parameter to "":

```
cluster1::> volume show -vserver vs1 -junction

Vserver  Volume  Active  Junction Path  Path Source
--------- ----------- -------- ---------------- ------------
vs1      data      true    /data            RW_volume
vs1      data1     true    /data/data1      RW_volume
vs1      data2     true    /data/data2      RW_volume
vs1      vs1_root  -       /                -

cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path /data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

Vserver: vs1
Share: data2
CIFS Server NetBIOS Name: VS1
Path: /data/data2
Share Properties: oplocks
continuously-available
Symlink Properties: -
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard
```
Adding the SeSecurityPrivilege privilege to the user account (for SQL Server of SMB shares)

The domain user account used for installing the SQL server must be assigned the “SeSecurityPrivilege” privilege to perform certain actions on the CIFS server that require privileges not assigned by default to domain users.

Before you begin
The domain account used for installing the SQL Server must already exist.

About this task
When adding the privilege to the SQL Server installer's account, Data ONTAP might validate the account by contacting the domain controller. The command might fail if Data ONTAP cannot contact the domain controller.

Steps
1. Add the “SeSecurityPrivilege” privilege:

   vserver cifs users-and-groups privilege add-privilege -vserver vserver_name -user-or-group-name account_name -privileges SeSecurityPrivilege

   The value for the -user-or-group-name parameter is the name of the domain user account used for installing the SQL Server.

2. Verify that the privilege is applied to the account:

   vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name account_name

Example

The following command adds the “SeSecurityPrivilege” privilege to the SQL Server installer's account in the EXAMPLE domain for Storage Virtual Machine (SVM) vs1:

   cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver vs1 -user-or-group-name EXAMPLE\SQLinstaller -privileges SeSecurityPrivilege

   cluster1::> vserver cifs users-and-groups privilege show -vserver vs1

<table>
<thead>
<tr>
<th>Vserver</th>
<th>User or Group Name</th>
<th>Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>EXAMPLE\SQLinstaller</td>
<td>SeSecurityPrivilege</td>
</tr>
</tbody>
</table>

Configuring the VSS shadow copy directory depth (for Hyper-V over SMB shares)

Optionally, you can configure the maximum depth of directories within SMB shares on which to create shadow copies. This parameter is useful if you want to manually control the maximum level of subdirectories on which Data ONTAP should create shadow copies.

Before you begin
The VSS shadow copy feature must be enabled.
About this task

The default is to create shadow copies for a maximum of five subdirectories. If the value is set to 0, Data ONTAP creates shadow copies for all subdirectories.

**Note:** Although you can specify that the shadow copy set directory depth include more than five subdirectories or all subdirectories, there is a Microsoft requirement that shadow copy set creation must be completed within 60 seconds. Shadow copy set creation fails if it cannot be completed within this time. The shadow copy directory depth you choose must not cause the creation time to exceed the time limit.

Steps

1. Set the privilege level to advanced:
   ```
   set -privilege advanced
   ```

2. Set the VSS shadow copy directory depth to the desired level:
   ```
   vserver cifs options modify -vserver vserver_name -shadowcopy-dir-depth integer
   ```

   **Example**
   ```
   vserver cifs options modify -vserver vs1 -shadowcopy-dir-depth 6
   ```

3. Return to the admin privilege level:
   ```
   set -privilege admin
   ```

Managing Hyper-V and SQL Server over SMB configurations

There are certain Data ONTAP tasks that you can perform to manage Hyper-V and SQL Server over SMB configurations.

Related tasks

*Creating Data ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server over SMB* on page 393

Configuring existing shares for continuous availability

You can modify existing shares to become continuously available shares that the Hyper-V and SQL Server application servers use to nondisruptively access Hyper-V virtual machine and configuration files and SQL Server database files.

About this task

You cannot use an existing share as a continuously available share for nondisruptive operations with application servers over SMB if the share has the following characteristics:

- If the homedirectory share property is set on that share
- If the share contains enabled symlinks or widelinks
- If the share contains junctioned volumes below the root of the share

You must verify that the two following share parameters are set correctly:

- The -offline-files parameter is set to either manual (the default) or none.
- Symlinks must be disabled.
The following share properties must be configured:

- continuously-available
- oplocks

The following share properties must not be set. If they are present in the list of current share properties, they need to be removed from the continuously available share:

- changenotify
- attributecache
- branchcache
- access-based-enumeration

Steps

1. Display the current share parameter settings and the current list of configured share properties:
   
   ```
   vserver cifs share show -vserver vserver_name -share-name share_name
   ```

2. If necessary, modify the share parameters to disable symlinks and set offline files to manual by using the `vserver cifs share properties modify` command.

   You can disable symlinks by setting the value of the `-symlink` parameter to "".

   - You can disable symlinks by setting the value of the `-symlink` parameter to "".
   - You can set the `-offline-files` parameter to the correct setting by specifying `manual`.

3. Add the `continuously-available` share property, and, if needed, the `oplocks` share property:

   ```
   vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties continuously-available[,oplock]
   ```

   If the `oplocks` share property is not already set, you must add it along with the `continuously-available` share property.

4. Remove any share properties that are not supported on continuously available shares:

   ```
   vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties properties[,....]
   ```

   You can remove one or more share properties by specifying the share properties with a comma-delimited list.

5. Verify that the `-symlink` and `-offline-files` parameters are set correctly:

   ```
   vserver cifs share show -vserver vserver_name -share-name share_name -fields symlink-properties,offline-files
   ```

6. Verify that the list of configured share properties is correct:

   ```
   vserver cifs shares properties show -vserver vserver_name -share-name share_name
   ```

Examples

The following example shows how to configure an existing share named “share1” on Storage Virtual Machine (SVM) vs1 for NDOs with an application server over SMB:

- Symlinks are disabled on the share by setting the `-symlink` parameter to "".
- The `-offline-file` parameter is modified and set to `manual`. 
• The continuously-available share property is added to the share.
• The oplocks share property is already in the list of share properties; therefore, it does not need to be added.
• The attributecache and changenotify share properties are removed from the share.
• The browsable share property is optional for a continuously available share used for NDOs with application servers over SMB and is retained as one of the share properties.

```bash
cluster1::> vserver cifs share show -vserver vs1 -share-name share1

Vserver: vs1
  Share: share1
  CIFS Server NetBIOS Name: vs1
  Path: /data
  Share Properties: oplocks
                    browsable
                    changenotify
                    attributecache
  Symlink Properties: enable
  File Mode Creation Mask: -
  Directory Mode Creation Mask: -
  Share Comment: -
  Share ACL: Everyone / Full Control
  File Attribute Cache Lifetime: 10s
  Volume Name: data
  Offline Files: documents
  Vscan File-Operations Profile: standard

cluster1::> vserver cifs share modify -vserver vs1 -share-name share1 -
  offline-file manual -symlink **

cluster1::> vserver cifs share properties add -vserver vs1 -share-name
  share1 -share-properties continuously-available

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
  share1 -share-properties attributecache,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name share1 -fields
  symlink-properties,offline-files
  vserver share-name symlink-properties offline-files
  -------- ------------------ -------------
  vs1 share1 -  manual

cluster1::> vserver cifs share properties show -vserver vs1 -share-name
  share1

  Vserver: vs1
  Share: share1
  Share Properties: oplocks
                   browsable
                   continuously-available
```

### Enabling or disabling VSS shadow copies for Hyper-V over SMB backups

If you use a VSS-aware backup application to back up Hyper-V virtual machine files stored on SMB shares, VSS shadow copy must be enabled. You can disable the VSS shadow copy if you do not use VSS-aware backup applications. The default is to enable the VSS shadow copy.

**About this task**

You can enable or disable VSS shadow copies at any time.

**Steps**

1. Set the privilege level to advanced:
   ```bash
   set -privilege advanced
   ```
2. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want VSS shadow copies to be...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>vserver cifs options modify -vserver vserver_name -shadowcopy-enabled true</td>
</tr>
<tr>
<td>Disabled</td>
<td>vserver cifs options modify -vserver vserver_name -shadowcopy-enabled false</td>
</tr>
</tbody>
</table>

3. Return to the admin privilege level:

```bash
set -privilege admin
```

Example

The following commands enable VSS shadow copies on SVM vs1:

```bash
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y
cluster1::*> vserver cifs options modify -vserver vs1 -shadowcopy-enabled true
cluster1::*> set -privilege admin
```

Considerations for reverting Hyper-V over SMB configurations

Before you revert to a Data ONTAP version that does not support nondisruptive operations for Hyper-V over SMB, you must be aware of certain considerations to ensure that you are prepared for the revert.

Before you revert, you must consider the following and take action where necessary:

- If you are reverting to a version of Data ONTAP that does not support SMB 3.0 and persistent handle locks, operations such as failover and giveback are disruptive because Hyper-V servers cannot reclaim disconnected durable handles.
- There must be no file access by the Hyper-V servers to virtual machine files when you revert:
  - You can use the Hyper-V application to migrate virtual machine files to another storage device or to local storage.
  - You can power down all virtual machines and manually terminate Hyper-V server connections to the data LIFs.
    Data ONTAP disables SMB 3.0 before reverting; therefore, if the SMB connections are not manually terminated, Data ONTAP terminates them during the revert.
- You cannot use the Hyper-V over SMB solution if you revert to a version of Data ONTAP that does not support it.
  You must configure the Hyper-V servers to use connected LUNs to store and access virtual machine files. You must then copy the virtual machine files from the SMB shares to the connected LUNs.
- To revert, there can be no ongoing Remote VSS shadow copy operations.
  If there are any, you must wait for the operations to finish or manually abort them before proceeding with the revert. If you need to abort any shadow copy operations, contact technical support for assistance. Upon a revert, Data ONTAP does not delete existing Snapshot copies.
Considerations for reverting SQL Server over SMB configurations

Before you revert to a Data ONTAP version that does not support nondisruptive operations for SQL Server over SMB shares, you must be aware of certain considerations to ensure that you are prepared for the revert.

Before you revert, you must consider the following and take action where necessary:

- If you are reverting to a version of Data ONTAP that does not support SMB 3.0 and persistent handle locks, operations such as failover and giveback are disruptive because SQL Server servers cannot reclaim disconnected durable handles.

- There must be no file access by the SQL Server servers to database files when you revert:
  - You can use the SQL Server application to migrate database files to another storage device or to local storage.
  - You can shut down all SQL Server databases and manually terminate SQL Server connections to the data LIFs.
    Data ONTAP disables SMB 3.0 before reverting; therefore, if the SMB connections are not manually terminated, Data ONTAP terminates them during the revert.

- You cannot use the SQL Server SMB 3.0 continuously available shares for nondisruptive operations if you revert to a version of Data ONTAP that does not support it.
  You must configure the SQL Server servers to use connected LUNs to store and access database files. You must then move the database files from the SMB shares to the connected LUNs.

Using statistics to monitor Hyper-V and SQL Server over SMB activity

You can display various CIFS and SMB statistics to monitor Hyper-V and SQL Server over SMB activity. For example, you can obtain information about the number of SMB sessions, the number of sessions from clients with continuously available capability, and the number of reconnection requests.

Related tasks

Determining whether SMB sessions are continuously available on page 415

Determining which statistics objects and counters are available

Before you can obtain information about CIFS, SMB, auditing, and BranchCache hash statistics and monitor performance, you must know which objects and counters are available from which you can obtain data.

Steps

1. Set the privilege level to advanced:
   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want to determine...</th>
<th>Enter...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Which objects are available</td>
<td>statistics catalog object show</td>
</tr>
</tbody>
</table>
If you want to determine... Enter...

Specific objects that are available statistics catalog object show -object object_name

Which counters are available statistics catalog counter show -object object_name

See the man pages for more information about which objects and counters are available.

3. Return to the admin privilege level:

set -privilege admin

Examples

The following command displays descriptions of selected statistic objects related to CIFS and SMB access in the cluster as seen at the advanced privilege level:

```bash
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.
Do you want to continue? [y|n]: y

cluster1::> statistics catalog object show -object audit
audit_ng                    CM object for exporting audit_ng performance counters

cluster1::> statistics catalog object show -object cifs
cifs                        The CIFS object reports activity of the Common Internet File System protocol subsystem. This is the Microsoft file-sharing protocol that evolved from the Server Message Block (SMB) application layer network protocol to connect PCs to Network Attached Storage devices (NAS). This object reports activity for both SMB and SMB2 revisions of the CIFS protocol. For information related only to SMB, see the 'smb1' object. For information related only to SMB2, see the 'smb2' object.

cluster1::> statistics catalog object show -object nblade_cifs
nblade_cifs                 The Common Internet File System (CIFS) protocol is an implementation of the Server Message Block (SMB) protocol. It is a standard application layer file system protocol used to share files with Windows(TM) systems. This object tracks the data transfer performance at the CIFS protocol layer, in Ontap's Nblade network component. These counters are relevant to the entire node, rather than individual virtual servers.

cluster1::> statistics catalog object show -object smb1
smb1                        These counters report activity from the SMB revision of the protocol. For information specific to SMB2, see the 'smb2' object. To see an overview across both revisions, see the 'cifs' object.

cluster1::> statistics catalog object show -object smb2
smb2                        These counters report activity from the SMB2/SMB3 revision of the protocol. For information specific to SMB, see the 'smb1' object. To see an overview across all revisions, see the 'cifs' object.

cluster1::> statistics catalog object show -object hashd
hashd                       The hashd object provides counters to measure the performance of the BranchCache hash daemon.
```

The following command displays information about some of the counters for the cifs object as seen at the advanced privilege level:

**Note:** This example does not display all of the available counters for the cifs object; output is truncated.
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>active_searches</td>
<td>Number of active searches over SMB and SMB2</td>
</tr>
<tr>
<td>auth_reject_too_many</td>
<td>Authentication refused after too many requests were made in rapid succession</td>
</tr>
<tr>
<td>avg_directory_depth</td>
<td>Average number of directories crossed by SMB and SMB2 path-based commands</td>
</tr>
<tr>
<td>avg_junction_depth</td>
<td>Average number of junctions crossed by SMB and SMB2 path-based commands</td>
</tr>
<tr>
<td>branchcache_hash_fetch_fail</td>
<td>Total number of times a request to fetch hash data failed. These are failures when attempting to read existing hash data. It does not include attempts to fetch hash data that has not yet been generated.</td>
</tr>
<tr>
<td>branchcache_hash_fetch_ok</td>
<td>Total number of times a request to fetch hash data succeeded.</td>
</tr>
<tr>
<td>branchcache_hash_sent_bytes</td>
<td>Total number of bytes sent to clients requesting hashes.</td>
</tr>
<tr>
<td>branchcache_missing_hash_bytes</td>
<td>Total number of bytes of data that had to be read by the client because the hash for that content was not available on the server.</td>
</tr>
<tr>
<td>change_notifications_outstanding</td>
<td>Number of active change notifications over SMB and SMB2</td>
</tr>
<tr>
<td>cifs_latency</td>
<td>Average latency for CIFS operations</td>
</tr>
<tr>
<td>cifs_latency_base</td>
<td>Total observed CIFS operations to be used as a base counter for CIFS average latency calculation</td>
</tr>
<tr>
<td>cifs_ops</td>
<td>Total number of CIFS operations</td>
</tr>
<tr>
<td>cifs_read_ops</td>
<td>Total number of CIFS read operations</td>
</tr>
<tr>
<td>cifs_write_ops</td>
<td>Total number of CIFS write operations</td>
</tr>
</tbody>
</table>

Related tasks

Displaying statistics on page 305

Related information

Clustered Data ONTAP 8.3.1 man page: statistics catalog object show - Display the list of objects
Clustered Data ONTAP 8.3.1 man page: statistics catalog counter show - Display the list of counters in an object

Displaying SMB statistics

You can display various SMB statistics to monitor performance and diagnose issues.

Steps

1. Use the statistics start and optional statistics stop commands to collect a data sample.
   
   For more information about these commands, see the Clustered Data ONTAP System Administration Guide for Cluster Administrators.

2. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want to display statistics for...</th>
<th>Enter the following command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>All versions of SMB</td>
<td>statistics show -object cifs</td>
</tr>
</tbody>
</table>
If you want to display statistics for...

<table>
<thead>
<tr>
<th>SMB 1.0</th>
<th>statistics show -object smb1</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMB 2.x and SMB 3.0</td>
<td>statistics show -object smb2</td>
</tr>
<tr>
<td>CIFS subsystem of the node</td>
<td>statistics show -object nblade_cifs</td>
</tr>
</tbody>
</table>

See the man page for more information.

Verifying that the configuration is capable of nondisruptive operations

You can verify that the Hyper-V or SQL Server over SMB configuration is healthy and able to perform operations nondisruptively by displaying health monitor information, verifying that the SMB shares are shared persistently, and by verifying the status of the LIF configuration.

How to use health monitoring to determine whether nondisruptive operation status is healthy

Health monitoring provides information about system health status across the cluster. The health monitor monitors Hyper-V and SQL Server over SMB configurations to ensure nondisruptive operations (NDOs) for the application servers. If the status is degraded, you can view details about the problem, including the probable cause and recommended recovery actions.

There are several health monitors. Data ONTAP monitors both overall system health and health for individual health monitors. The node connectivity health monitor contains the CIFS-NDO subsystem. The monitor has a set of health policies that trigger alerts if certain physical conditions can lead to disruption, and if a disruptive condition exists, generates alerts and provides information about corrective actions. For NDO over SMB configurations, alerts are generated for the two following conditions:

<table>
<thead>
<tr>
<th>Alert ID</th>
<th>Severity</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>HaNotReadyCifsNdo_Alert</td>
<td>Major</td>
<td>One or more files hosted by a volume in an aggregate on the node have been opened through a continuously available SMB share with the promise of persistence in the event of a failure; however, the HA relationship with the partner is either not configured or not healthy.</td>
</tr>
<tr>
<td>NoStandbyLifCifsNdo_Alert</td>
<td>Minor</td>
<td>The Storage Virtual Machine (SVM) is actively serving data over SMB through a node, and there are SMB files opened persistently over continuously available shares; however, its partner node is not exposing any active data LIFs for the SVM.</td>
</tr>
</tbody>
</table>
Displaying nondisruptive operation status by using system health monitoring

You can use the `system health` commands to display information about the overall system health of the cluster and the health of the CIFS-NDO subsystem, to respond to alerts, to configure future alerts, and to display information about how health monitoring is configured.

**About this task**

For more information about using system health monitoring, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators.*

**Steps**

1. Monitor health status by performing the appropriate action:

<table>
<thead>
<tr>
<th>If you want to display...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>The health status of the system, which reflects the overall status of individual health monitors</td>
<td><code>system health status show</code></td>
</tr>
<tr>
<td>Information about the health status of the CIFS-NDO subsystem</td>
<td><code>system health subsystem show -subsystem CIFS-NDO -instance</code></td>
</tr>
</tbody>
</table>

2. Display information about how CIFS-NDO alert monitoring is configured by performing the appropriate actions:

<table>
<thead>
<tr>
<th>If you want to display information about...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>The configuration and status of the health monitor for the CIFS-NDO subsystem, such as nodes monitored, initialization state, and status</td>
<td><code>system health config show -subsystem CIFS-NDO</code></td>
</tr>
<tr>
<td>The CIFS-NDO alerts that a health monitor can potentially generate</td>
<td><code>system health alert definition show -subsystem CIFS-NDO</code></td>
</tr>
<tr>
<td>CIFS-NDO health monitor policies, which determine when alerts are raised</td>
<td><code>system health policy definition show -monitor node-connect</code></td>
</tr>
</tbody>
</table>

**Note:** Use the `-instance` parameter to display detailed information.

**Examples**

The following output shows information about the overall health status of the cluster and the CIFS-NDO subsystem:

```
cluster1:~> system health status show
Status
-------
ok
cluster1:~> system health subsystem show -instance -subsystem CIFS-NDO
Subsystem: CIFS-NDO
```
Verifying the continuously available SMB share configuration

To support nondisruptive operations, Hyper-V and SQL Server SMB shares must be configured as continuously available shares. Additionally, there are certain other share settings that you must check. You should verify that the shares are properly configured to ensure seamless nondisruptive operations for the application servers if there are planned or unplanned disruptive events.

About this task

You must verify that the two following share parameters are set correctly:

- The `-offline-files` parameter is set to either `manual` (the default) or `none`.
- Symmlinks must be disabled.

To ensure proper nondisruptive operations, the following share properties must be set:

- `continuously-available`
- `oplocks`

The following share properties must not be set:

- `homedirectory`
- `changefile`
- `attributecache`
- `branchcache`
- `access-based-encryption`
Steps

1. Verify that the offline files are set to manual or disabled and that symlinks are disabled:
   
   \[ \text{vserver cifs shares show \text{-vserver} vserver\_name} \]

2. Verify that the SMB shares are configured for continuous availability:
   
   \[ \text{vserver cifs shares properties show \text{-vserver} vserver\_name} \]

Examples

The following example displays the share setting for a share named “share1” on Storage Virtual Machine (SVM, formerly known as Vserver) vs1. Offline files are set to manual and symlinks are disabled (designated by a hyphen in the Symlink Properties field output):

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1
Vserver: vs1
Share: share1
CIFS Server NetBIOS Name: VS1
Path: /data/share1
Share Properties: oplocks
                 continuously-available
Symlink Properties: -
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard
```

The following example displays the share properties for a share named “share1” on SVM vs1:

```
cluster1::> vserver cifs share properties show -vserver vs1 -share-name share1
Vserver    Share   Properties
---------  ------  ----------
vs1        share1  oplocks
           continuously-available
```

Verifying LIF status

Even if you configure Storage Virtual Machines (SVMs) with Hyper-V and SQL Server over SMB configurations to have LIFs on each node in a cluster, during day-to-day operations, some LIFs might move to ports on another node. You must verify LIF status and take any necessary corrective actions.

About this task

To provide seamless, nondisruptive operation support, each node in a cluster must have at least one LIF for the SVM, and all the LIFs must be associated with a home port. If some of the configured LIFs are not currently associated with their home port, you must fix any port issues and then revert the LIFs to their home port.

Steps

1. Display information about configured LIFs for the SVM:
   
   \[ \text{network interface show \text{-vserver} vserver\_name} \]

Example

In this example, “lif1” is not located on the home port.
network interface show -vserver vs1

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Logical Interface</th>
<th>Status</th>
<th>Network Address/Mask</th>
<th>Current Node</th>
<th>Current Port</th>
<th>Home</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>lif1</td>
<td>up/up</td>
<td>10.0.0.128/24</td>
<td>node2</td>
<td>e0d</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td>lif2</td>
<td>up/up</td>
<td>10.0.0.129/24</td>
<td>node2</td>
<td>e0d</td>
<td>true</td>
</tr>
</tbody>
</table>

2. If some of the LIFs are not on their home ports, perform the following steps:

a. For each LIF, determine what the LIF's home port is:

   ```
   network interface show -vserver vserver_name -lif lif_name -fields home-node,home-port
   ```

   Example

   ```
   network interface show -vserver vs1 -lif lif1 -fields home-node,home-port
   ```

<table>
<thead>
<tr>
<th>vserver</th>
<th>lif</th>
<th>home-node</th>
<th>home-port</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>lif1</td>
<td>node1</td>
<td>e0d</td>
</tr>
</tbody>
</table>

b. For each LIF, determine whether the LIF's home port is up:

   ```
   network port show -node node_name -port port -fields port,link
   ```

   Example

   ```
   network port show -node node1 -port e0d -fields port,link
   ```

<table>
<thead>
<tr>
<th>node</th>
<th>port</th>
<th>link</th>
</tr>
</thead>
<tbody>
<tr>
<td>node1</td>
<td>e0d</td>
<td>up</td>
</tr>
</tbody>
</table>

   In this example, “lif1” should be migrated back to its home port, `node1:e0d`.

3. If any of the home port network interfaces to which the LIFs should be associated are not in the `up` state, resolve the problem so that these interfaces are up.

4. If needed, revert the LIFs to their home ports:

   ```
   network interface revert -vserver vserver_name -lif lif_name
   ```

   Example

   ```
   network interface revert -vserver vs1 -lif lif1
   ```

5. Verify that each node in the cluster has an active LIF for the SVM:

   ```
   network interface show -vserver vserver_name
   ```

   Example

   ```
   network interface show -vserver vs1
   ```
<table>
<thead>
<tr>
<th>Vserver</th>
<th>Logical Interface</th>
<th>Status</th>
<th>Network Address/Mask</th>
<th>Current Node</th>
<th>Current Port</th>
<th>Current Is Home</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>lif1</td>
<td>up/up</td>
<td>10.0.0.128/24</td>
<td>node1</td>
<td>e0d</td>
<td>true</td>
</tr>
<tr>
<td></td>
<td>lif2</td>
<td>up/up</td>
<td>10.0.0.129/24</td>
<td>node2</td>
<td>e0d</td>
<td>true</td>
</tr>
</tbody>
</table>

### Related tasks

*Creating Data ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server over SMB* on page 393

### Determining whether SMB sessions are continuously available

You can display information about SMB sessions and SMB open files to determine whether they are continuously available.

### Related tasks

*Using statistics to monitor Hyper-V and SQL Server over SMB activity* on page 407

### Displaying SMB session information

You can display information about established SMB sessions, including the SMB connection and session ID and the IP address of the workstation using the session. You can display information about the session’s SMB protocol version and continuously available protection level, which helps you identify whether the session supports nondisruptive operations.

#### About this task

You can display information for all sessions on your Storage Virtual Machine (SVM) in summary form. However, in many cases, the amount of output returned is large. You can customize what information is displayed in the output by specifying optional parameters:

- You can use the optional `-fields` parameter to display output on the fields you choose.
  
  You can enter `-fields ?` to determine what fields you can use.

- You can use the `-instance` parameter to display detailed information about established SMB sessions.

- You can use the `-fields` parameter or the `-instance` parameter either alone or in combination with other optional parameters.

#### Step

1. Perform one of the following actions:

   **If you want to display SMB session information for established sessions...**
   Enter the following command...

<table>
<thead>
<tr>
<th>For all sessions on the SVM in summary form</th>
<th><code>vserver cifs session show -vserver vserver_name</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>On a specified connection ID</td>
<td><code>vserver cifs session show -vserver vserver_name -connection-id integer</code></td>
</tr>
<tr>
<td>From a specified workstation IP address</td>
<td><code>vserver cifs session show -vserver vserver_name -address workstation_IP_address</code></td>
</tr>
</tbody>
</table>
If you want to display SMB session information for established sessions...

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>On the specified LIF IP address</td>
<td><code>vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address</code></td>
</tr>
<tr>
<td>On a specified node</td>
<td>`vserver cifs session show -vserver vserver_name -node {node_name</td>
</tr>
<tr>
<td>From a specified Windows user</td>
<td><code>vserver cifs session show -vserver vserver_name -windows-user user_name</code></td>
</tr>
<tr>
<td></td>
<td>The format for <code>user_name</code> is <code>[domain]\user</code>.</td>
</tr>
<tr>
<td>With a specified authentication mechanism</td>
<td><code>vserver cifs session show -vserver vserver_name -auth-mechanism</code></td>
</tr>
<tr>
<td></td>
<td>The value for <code>-auth-mechanism</code> can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• NTLMv1</td>
</tr>
<tr>
<td></td>
<td>• NTLMv2</td>
</tr>
<tr>
<td></td>
<td>• Kerberos</td>
</tr>
<tr>
<td></td>
<td>• Anonymous</td>
</tr>
<tr>
<td>With the specified protocol version</td>
<td><code>vserver cifs session show -vserver vserver_name -protocol-version</code></td>
</tr>
<tr>
<td></td>
<td>The value for <code>-protocol-version</code> can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• SMB1</td>
</tr>
<tr>
<td></td>
<td>• SMB2</td>
</tr>
<tr>
<td></td>
<td>• SMB2_1</td>
</tr>
<tr>
<td></td>
<td>• SMB3</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Continuously available protection is available only on SMB 3.0 sessions. To see continuously available protection status on all qualifying sessions, specify this parameter with the value set to <code>SMB3</code>.</td>
</tr>
<tr>
<td>With the specified level of continuously available protection</td>
<td><code>vserver cifs session show -vserver vserver_name -continuously-available</code></td>
</tr>
<tr>
<td></td>
<td>The value for <code>-continuously-available</code> can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• No</td>
</tr>
<tr>
<td></td>
<td>• Yes</td>
</tr>
<tr>
<td></td>
<td>• Partial</td>
</tr>
</tbody>
</table>
|                                                                         | **Note**: If the continuously available status is `Partial`, this means that the session contains at least one open continuously available file, but the session has some files that are not open with continuously available protection. You can use the `vserver cifs sessions file show` command to determine which files on the established session are not open with continuously available protection.
If you want to display SMB session information for established sessions...
Enter the following command...

With the specified SMB signing session status  

```
vserver cifs session show -vserver vserver_name -is-session-signed {true|false}
```

### Examples

The following command displays session information on SVM sessions vs1 established from a workstation with the IP address of 10.1.1.1:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node: node1
Vserver: vs1
Connection Session
ID        ID      Workstation     Windows User    Files     Time
---------- ------- ---------------- ------------- ------- ------------
3151272279 1       10.1.1.1         DOMAIN\joe          2          23s
```

The following command displays detailed session information on sessions with continuously available protection on SVM vs1. The connection was made by using the domain computer-machine account.

```
cluster1::> vserver cifs session show -instance -continuously-available Yes
Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation IP address: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\SERVER1$
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: Yes
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted
```

The following command displays session information on sessions using SMB 3.0 on SVM vs1. The user connected to this share from an SMB 3.0 capable client by using the LIF IP address; therefore, the authentication mechanism defaulted to NTLMv2. The connection must be made using Kerberos authentication to connect with continuously available protection.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3
Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 3151272607
Incoming Data LIF IP Address: 10.2.1.2
Workstation IP address: 10.1.1.3
Authentication Mechanism: NTLMv2
Windows User: DOMAIN\administrator
UNIX User: pcuser
Open Shares: 1
Open Files: 0
Open Other: 0
Connected Time: 6m 22s
Idle Time: 5m 42s
Protocol Version: SMB3
Continuously Available: No
Displaying information about open SMB files

You can display information about open SMB files, including the SMB connection and session ID, the hosting volume, the share name, and the share path. You can display information about a file’s continuously available protection level, which is helpful in determining whether an open file is in a state that supports nondisruptive operations.

About this task

You can display information about open files on an established SMB session. The displayed information is useful when you need to determine SMB session information for particular files within an SMB session.

For example, if you have an SMB session where some of the open files are open with continuously available protection and some are not open with continuously available protection (the value for the -continuously-available field in vserver cifs session show command output is Partial), you can determine which files are not continuously available by using this command.

You can display information for all open files on established SMB sessions on Storage Virtual Machines (SVMs) in summary form by using the vserver cifs session file show command without any optional parameters.

However, in many cases, the amount of output returned is large. You can customize what information is displayed in the output by specifying optional parameters. This can be helpful when you want to view information for only a small subset of open files.

- You can use the optional -fields parameter to display output on the fields you choose.
  You can use this parameter either alone or in combination with other optional parameters.

- You can use the -instance parameter to display detailed information about open SMB files.
  You can use this parameter either alone or in combination with other optional parameters.

Step

1. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If you want to display open SMB files...</th>
<th>Enter the following command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>On the SVM in summary form</td>
<td>vserver cifs session file show -vserver vserver_name</td>
</tr>
<tr>
<td>On a specified node</td>
<td>vserver cifs session file show -vserver vserver_name -node (node_name</td>
</tr>
<tr>
<td>On a specified file ID</td>
<td>vserver cifs session file show -vserver vserver_name -file-id integer</td>
</tr>
<tr>
<td>On a specified SMB connection ID</td>
<td>vserver cifs session file show -vserver vserver_name -connection-id integer</td>
</tr>
<tr>
<td>On a specified SMB session ID</td>
<td>vserver cifs session file show -vserver vserver_name -session-id integer</td>
</tr>
<tr>
<td>On the specified hosting aggregate</td>
<td>vserver cifs session file show -vserver vserver_name -hosting-aggregate aggregate_name</td>
</tr>
</tbody>
</table>
If you want to display open SMB files...
Enter the following command...

<table>
<thead>
<tr>
<th>On the specified volume</th>
<th><code>vserver cifs session file show -vserver vserver_name -hosting-volume volume_name</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>On the specified SMB share</td>
<td><code>vserver cifs session file show -vserver vserver_name -share share_name</code></td>
</tr>
<tr>
<td>On the specified SMB path</td>
<td><code>vserver cifs session file show -vserver vserver_name -path path</code></td>
</tr>
<tr>
<td>With the specified level of continuously available protection</td>
<td><code>vserver cifs session file show -vserver vserver_name -continuously-available continuously_available_status</code></td>
</tr>
</tbody>
</table>

The value for `continuously-available` can be one of the following:

- **No**
- **Yes**

**Note:** If the continuously available status is **No**, this means that these open files are not capable of nondisruptively recovering from takeover and giveback. They also cannot recover from general aggregate relocation between partners in a high-availability relationship.

<table>
<thead>
<tr>
<th>With the specified reconnected state</th>
<th><code>vserver cifs session file show -vserver vserver_name -reconnected reconnected_state</code></th>
</tr>
</thead>
</table>

The value for `reconnected` can be one of the following:

- **No**
- **Yes**

**Note:** If the reconnected state is **No**, the open file is not reconnected after a disconnection event. This can mean that the file was never disconnected, or that the file was disconnected and is not successfully reconnected. If the reconnected state is **Yes**, this means that the open file is successfully reconnected after a disconnection event.

There are additional optional parameters that you can use to refine the output results. See the man page for more information.

### Examples

The following example displays information about open files on SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1

File    File      Open Hosting               Continuously
ID      Type      Mode Volume    Share       Available
------- --------- ---- --------- ----------- ------------
41      Regular   r    data      data        Yes
Path: \\mytest.rtf
```

The following example displays detailed information about open SMB files with file ID 82 on SVM vs1:

```
```
```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82 -instance

<table>
<thead>
<tr>
<th>Node</th>
<th>node1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vserver</td>
<td>vs1</td>
</tr>
<tr>
<td>File ID</td>
<td>82</td>
</tr>
<tr>
<td>Connection ID</td>
<td>104617</td>
</tr>
<tr>
<td>Session ID</td>
<td>1</td>
</tr>
<tr>
<td>File Type</td>
<td>Regular</td>
</tr>
<tr>
<td>Open Mode</td>
<td>rw</td>
</tr>
<tr>
<td>Aggregate Hosting File</td>
<td>aggr1</td>
</tr>
<tr>
<td>Volume Hosting File</td>
<td>data1</td>
</tr>
<tr>
<td>CIFS Share</td>
<td>data1</td>
</tr>
<tr>
<td>Path from CIFS Share</td>
<td>windows\win8\test\test.txt</td>
</tr>
<tr>
<td>Share Mode</td>
<td>rw</td>
</tr>
<tr>
<td>Range Locks</td>
<td>1</td>
</tr>
<tr>
<td>Continuously Available</td>
<td>Yes</td>
</tr>
<tr>
<td>Reconnected</td>
<td>No</td>
</tr>
</tbody>
</table>
```
Auditing NAS events on SVMs with FlexVol volumes

Auditing for NAS events is a security measure that enables you to track and log certain CIFS and NFS events on Storage Virtual Machines (SVMs) with FlexVol volumes. This helps you track potential security problems and provides evidence of any security breaches. You can also stage and audit Active Directory central access policies to see what the result of implementing them would be.

CIFS events

You can audit the following events:

- SMB file and folder access events
  You can audit SMB file and folder access events on objects stored on FlexVol volumes belonging to the auditing-enabled SVMs.

- CIFS logon and logoff events
  You can audit CIFS logon and logoff events for CIFS servers on SVMs with FlexVol volumes.

- Central access policy staging events
  You can audit the effective access of objects on CIFS servers using permissions applied through proposed central access policies. Auditing through the staging of central access policies enables you to see what the effects are of central access policies before they are deployed.

  Auditing of central access policy staging is set up using Active Directory GPOs; however, the SVM auditing configuration must be configured to audit central access policy staging events. Although you can enable central access policy staging in the auditing configuration without enabling Dynamic Access Control on the CIFS server, central access policy staging events are generated only if Dynamic Access Control is enabled. Dynamic Access Control is enabled through a CIFS server option. It is not enabled by default.

NFS events

You can audit file and directory NFSv4 access events on objects stored on SVMs with FlexVol volumes.

Related concepts

- Securing file access by using file permissions on page 190
- SMB events that can be audited on page 426
- Securing file access by using Dynamic Access Control (DAC) on page 196

How auditing works

Before you plan and configure your auditing configuration, you should understand how auditing works.

Basic auditing concepts

To understand auditing in Data ONTAP, you should be aware of some basic auditing concepts.

Staging files

The intermediate binary files on individual nodes where audit records are stored prior to consolidation and conversion. Staging files are contained in staging volumes.
Staging volume

A dedicated volume created by Data ONTAP to store staging files. There is one staging volume per aggregate. Staging volumes are shared by all audit-enabled Storage Virtual Machines (SVMs) to store audit records of data access for data volumes in that particular aggregate. Each SVM's audit records are stored in a separate directory within the staging volume.

Cluster administrators can view information about staging volumes, but most other volume operations are not permitted. Only clustered Data ONTAP can create staging volumes. Clustered Data ONTAP automatically assigns a name to staging volumes. All staging volume names begin with `MDV_aud_` followed by the UUID of the aggregate containing that staging volume (for example: `MDV_aud_1d0131843d4811e296fc123478563412`).

System volumes

A FlexVol volume that contains special metadata, such as metadata for file services audit logs. The admin SVM owns system volumes, which are visible across the cluster. Staging volumes are a type of system volume.

Consolidation task

A task that gets created when auditing is enabled. This long-running task on each SVM takes the audit records from staging files across the member nodes of the SVM. This task merges the audit records in sorted chronological order, and then converts them to a user-readable event log format specified in the auditing configuration—either the EVTX or XML file format. The converted event logs are stored in the audit event log directory that is specified in the SVM auditing configuration.

How the Data ONTAP auditing process works

The Data ONTAP auditing process is different than the Microsoft auditing process. Before you configure auditing, you should understand how the Data ONTAP auditing process works.

Audit records are initially stored in binary staging files on individual nodes. If auditing is enabled on an SVM, every member node maintains staging files for that SVM. Periodically, they are consolidated and converted to user-readable event logs, which are stored in the audit event log directory for the SVM.

Process when auditing is enabled on an SVM

Auditing can only be enabled on SVMs with FlexVol volumes. When the storage administrator enables auditing on the SVM, the auditing subsystem checks whether staging volumes are present. A staging volume must exist for each aggregate that contains data volumes owned by the SVM. The auditing subsystem creates any needed staging volumes if they do not exist.

The auditing subsystem also completes other prerequisite tasks before auditing is enabled:

- The auditing subsystem verifies that the log directory path is available and does not contain symlinks.
  The log directory must already exist. The auditing subsystem does not assign a default log file location. If the log directory path specified in the auditing configuration is not a valid path, auditing configuration creation fails with the following error:
  
  ```
  The specified path "<path>" does not exist in the namespace belonging to Vserver "<Vserver_name>"
  ```
  Configuration creation fails if the directory exists but contains symlinks.

- Auditing schedules the consolidation task.

After this task is scheduled, auditing is enabled. The SVM auditing configuration and the log files persist across a reboot or if the NFS or CIFS servers are stopped or restarted.
**Event log consolidation**

Log consolidation is a scheduled task that runs on a routine basis until auditing is disabled. When auditing is disabled, the consolidation task ensures that all the remaining logs are consolidated.

**Guaranteed auditing**

By default, auditing is guaranteed. Data ONTAP guarantees that all auditable file access events (as specified by configured audit policy ACLs) are recorded, even if a node is unavailable. A requested file operation cannot be completed until the audit record for that operation is saved to the staging volume on persistent storage. If audit records cannot be committed to the disk in the staging files, either because of insufficient space or because of other issues, client operations are denied.

**Consolidation process when a node is unavailable**

If a node containing volumes belonging to an SVM with auditing enabled is unavailable, the behavior of the auditing consolidation task depends on whether the node's SFO partner (or the HA partner in the case of a two-node cluster) is available.

- If the staging volume is available through the SFO partner, the staging volumes last reported from the node are scanned, and consolidation proceeds normally.

- If the SFO partner is not available, the task creates a partial log file.

  When a node is not reachable, the consolidation task consolidates the audit records from the other available nodes of that SVM. To identify that it is not complete, the task adds the suffix `.partial` to the consolidated file name.

- After the unavailable node is available, the audit records in that node are consolidated with the audit records from the other nodes at that point of time.

- All audit records are preserved.

**Event log rotation**

Audit event log files are rotated when they reach a configured threshold log size or on a configured schedule. When an event log file is rotated, the scheduled consolidation task first renames the active converted file to a time-stamped archive file, and then creates a new active converted event log file.

**Process when auditing is disabled on the SVM**

When auditing is disabled on the SVM, the consolidation task is triggered one final time. All outstanding, recorded audit records are logged in user-readable format. Existing event logs stored in the event log directory are not deleted when auditing is disabled on the SVM and are available for viewing.

After all existing staging files for that SVM are consolidated, the consolidation task is removed from the schedule. Disabling the auditing configuration for the SVM does not remove the auditing configuration. A storage administrator can reenable auditing at any time.

The auditing consolidation job, which gets created when auditing is enabled, monitors the consolidation task and re-creates it if the consolidation task exits because of an error. Previously, users could delete the auditing consolidation job by using job manager commands such as `job delete`. Users are no longer allowed to delete the auditing consolidation job.

**Related concepts**

- [Basic auditing concepts](#) on page 421
- [What the supported audit event log formats are](#) on page 425
- [SMB events that can be audited](#) on page 426
Aggregate space considerations when enabling auditing

When an auditing configuration is created and auditing is enabled on at least one Storage Virtual Machine (SVM) in the cluster, the auditing subsystem creates staging volumes on all existing aggregates and on all new aggregates that are created. You need to be aware of certain aggregate space considerations when you enable auditing on the cluster.

Staging volume creation might fail due to non-availability of space in an aggregate. This might happen if you create an auditing configuration and existing aggregates do not have enough space to contain the staging volume.

You should ensure that there is enough space on existing aggregates for the staging volumes before enabling auditing on an SVM.

Auditing requirements and considerations

Before you configure and enable auditing on your Storage Virtual Machine (SVM), you need to be aware of certain requirements and considerations.

- The maximum number of auditing-enabled SVMs supported in a cluster is 50.
- Auditing is not tied to CIFS or NFS licensing.
  You can configure and enable auditing even if CIFS and NFS licenses are not installed on the cluster.
- NFS auditing supports security ACEs (type U).
- For NFS auditing, there is no mapping between mode bits and auditing ACEs.
  When converting ACLs to mode bits, auditing ACEs are skipped. When converting mode bits to ACLs, auditing ACEs are not generated.
- The directory specified in the auditing configuration must exist.
  If it does not exist, the command to create the auditing configuration fails.
- The directory specified in the auditing configuration must meet the following requirements:
  - The directory must not contain symbolic links.
    If the directory specified in the auditing configuration contains symbolic links, the command to create the auditing configuration fails.
  - You must specify the directory by using an absolute path.
    You should not specify a relative path, for example, `/vs1/../`
- Auditing is dependent on having available space in the staging volumes.
  You must be aware of and have a plan for ensuring that there is sufficient space for the staging volumes in aggregates that contain audited volumes.
- Auditing is dependent on having available space in the volume containing the directory where converted event logs are stored.
You must be aware of and have a plan for ensuring that there is sufficient space in the volumes used to store event logs. You can specify the number of event logs to retain in the auditing directory by using the `-rotate-limit` parameter when creating an auditing configuration, which can help to ensure that there is enough available space for the event logs in the volume.

- Although you can enable central access policy staging in the auditing configuration without enabling Dynamic Access Control on the CIFS server, Dynamic Access Control must be enabled to generate central access policy staging events. Dynamic Access Control is not enabled by default.

**Related concepts**

*Planning the auditing configuration* on page 431

**What the supported audit event log formats are**

Supported file formats for the converted audit event logs are `EVTX` and `XML` file formats.

You can specify the type of file format when you create the auditing configuration. By default, Data ONTAP converts the binary logs to the `EVTX` file format.

**Related concepts**

*Viewing audit event logs* on page 425

*How active audit logs are viewed using Event Viewer* on page 426

**Viewing audit event logs**

You can use audit event logs to determine whether you have adequate file security and whether there have been improper file and folder access attempts. You can view and process audit event logs saved in the `EVTX` or `XML` file formats.

- **EVTX file format**
  
  You can open the converted `EVTX` audit event logs as saved files using Microsoft Event Viewer. There are two options that you can use when viewing event logs using Event Viewer:

  - General view
    
    Information that is common to all events is displayed for the event record. In this version of Data ONTAP, the event-specific data for the event record is not displayed. You can use the detailed view to display event-specific data.

  - Detailed view
    
    A friendly view and a XML view are available. The friendly view and the XML view display both the information that is common to all events and the event-specific data for the event record.

- **XML file format**

  You can view and process `XML` audit event logs on third-party applications that support the `XML` file format. XML viewing tools can be used to view the audit logs provided you have the XML schema and information about definitions for the XML fields. For more information about obtaining the XML schema and documents related to XML definitions, contact technical support or your account team.

**Related concepts**

*How the Data ONTAP auditing process works* on page 422

*How active audit logs are viewed using Event Viewer* on page 426
How active audit logs are viewed using Event Viewer

If the audit consolidation process is running on the cluster, the consolidation process appends new records to the active audit log file for audit-enabled Storage Virtual Machines (SVMs). This active audit log can be accessed and opened over an SMB share in Microsoft Event Viewer.

In addition to viewing existing audit records, Event Viewer has a refresh option that enables you to refresh the content in the console window. Whether the newly appended logs are viewable in Event Viewer depends on whether oplocks are enabled on the share used to access the active audit log.

<table>
<thead>
<tr>
<th>Oplocks setting on the share</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Event Viewer opens the log that contains events written to it up to that point in time. The refresh operation does not refresh the log with new events appended by the consolidation process.</td>
</tr>
<tr>
<td>Disabled</td>
<td>Event Viewer opens the log that contains events written to it up to that point in time. The refresh operation refreshes the log with new events appended by the consolidation process.</td>
</tr>
</tbody>
</table>

Note: This information is applicable only for EVTX event logs. XML event logs can be viewed through SMB in a browser or through NFS using any XML editor or viewer.

SMB events that can be audited

Data ONTAP can audit certain SMB events, including certain file and folder access events, certain logon and logoff events, and central access policy staging events. Knowing which access events can be audited is helpful when interpreting results from the event logs.

The following SMB events can be audited:

<table>
<thead>
<tr>
<th>Event ID (EVT/EVTX)</th>
<th>Event</th>
<th>Description</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>540/4624</td>
<td>An account was successfully logged on</td>
<td>LOGON/LOGOFF: Network (CIFS) logon.</td>
<td>Logon and Logoff</td>
</tr>
<tr>
<td>529/4625</td>
<td>An account failed to log on</td>
<td>LOGON/LOGOFF: Unknown user name or bad password.</td>
<td>Logon and Logoff</td>
</tr>
<tr>
<td>530/4625</td>
<td>An account failed to log on</td>
<td>LOGON/LOGOFF: Account logon time restriction.</td>
<td>Logon and Logoff</td>
</tr>
<tr>
<td>531/4625</td>
<td>An account failed to log on</td>
<td>LOGON/LOGOFF: Account currently disabled.</td>
<td>Logon and Logoff</td>
</tr>
<tr>
<td>532/4625</td>
<td>An account failed to log on</td>
<td>LOGON/LOGOFF: User account has expired.</td>
<td>Logon and Logoff</td>
</tr>
<tr>
<td>Event ID (EVT/EVTX)</td>
<td>Event</td>
<td>Description</td>
<td>Category</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td>533/4625</td>
<td>An account failed to log on</td>
<td>LOGON/LOGOFF: User cannot log on to this computer.</td>
<td>Logon and Logoff</td>
</tr>
<tr>
<td>534/4625</td>
<td>An account failed to log on</td>
<td>LOGON/LOGOFF: User not granted logon type here.</td>
<td>Logon and Logoff</td>
</tr>
<tr>
<td>535/4625</td>
<td>An account failed to log on</td>
<td>LOGON/LOGOFF: User's password has expired.</td>
<td>Logon and Logoff</td>
</tr>
<tr>
<td>537/4625</td>
<td>An account failed to log on</td>
<td>LOGON/LOGOFF: Logon failed for reasons other than above.</td>
<td>Logon and Logoff</td>
</tr>
<tr>
<td>539/4625</td>
<td>An account failed to log on</td>
<td>LOGON/LOGOFF: Account locked out.</td>
<td>Logon and Logoff</td>
</tr>
<tr>
<td>538/4634</td>
<td>An account was logged off</td>
<td>LOGON/LOGOFF: Local or network user logoff.</td>
<td>Logon and Logoff</td>
</tr>
<tr>
<td>560/4656</td>
<td>Open Object/Create Object</td>
<td>OBJECT ACCESS: Object (file or directory) open.</td>
<td>File Access</td>
</tr>
<tr>
<td>563/4659</td>
<td>Open Object with the Intent to Delete</td>
<td>OBJECT ACCESS: A handle to an object (file or directory) was requested with the Intent to Delete.</td>
<td>File Access</td>
</tr>
<tr>
<td>564/4660</td>
<td>Delete Object</td>
<td>OBJECT ACCESS: Delete Object (file or directory). Data ONTAP generates this event when a Windows client attempts to delete the object (file or directory).</td>
<td>File Access</td>
</tr>
<tr>
<td>567/4663</td>
<td>Read Object/Write Object/Get Object Attributes/Set Object Attributes</td>
<td>OBJECT ACCESS: Object access attempt (read, write, get attribute, set attribute). <strong>Note:</strong> For this event, Data ONTAP audits only the first SMB read and first SMB write operation (success or failure) on an object. Data ONTAP prevents excessive log entries when a single client opens an object and performs many successive read or write operations to the same object.</td>
<td>File Access</td>
</tr>
<tr>
<td>NA/4664</td>
<td>Hard link</td>
<td>OBJECT ACCESS: An attempt was made to create a hard link.</td>
<td>File Access</td>
</tr>
<tr>
<td>NA/4818</td>
<td>Proposed central access policy does not grant the same access permissions as the current central access policy</td>
<td>OBJECT ACCESS: Central Access Policy Staging.</td>
<td>File Access</td>
</tr>
<tr>
<td>NA/NA Data ONTAP Event ID 9999</td>
<td>Rename Object</td>
<td>OBJECT ACCESS: Object renamed. This is a Data ONTAP event. It is not currently supported by Windows as a single event.</td>
<td>File Access</td>
</tr>
</tbody>
</table>
### Additional information about Event 4656

The `HandleID` tag in the audit XML event contains the handle of the object (file or directory) accessed. The `HandleID` tag for the EVTX 4656 event contains different information depending on whether the open event is for creating a new object or for opening an existing object:

- If the open event is an open request to create a new object (file or directory), the `HandleID` tag in the audit XML event shows an empty `HandleID` (for example: `<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>`).
  
  The `HandleID` is empty because the OPEN (for creating a new object) request gets audited before the actual object creation happens and before a handle exists. Subsequent audited events for the same object have the right object handle in the `HandleID` tag.

- If the open event is an open request to open an existing object, the audit event will have the assigned handle of that object in the `HandleID` tag (for example: `<Data Name="HandleID">00000000000401;00;000000ea;00123ed4</Data>`).

### Related concepts

- [Configuring audit policies on NTFS security-style files and directories](#) on page 439

### Related tasks

- [Determining what the complete path to the audited object is](#) on page 428

### Determining what the complete path to the audited object is

The object path printed in the `<ObjectName>` tag for an audit record contains the name of the volume (in parentheses) and the relative path from the root of the containing volume. If you want to determine the complete path of the audited object, including the junction path, there are certain steps you must take.

#### Steps

1. Determine what the volume name and relative path to audited object is by looking at the `<ObjectName>` tag in the audit event.

   **Example**

   In this example, the volume name is “data1” and the relative path to the file is `/dir1/file.txt:
   
   `<Data Name="ObjectName">(data1);/dir1/file.txt</Data>`

2. Using the volume name determined in the previous step, determine what the junction path is for the volume containing the audited object:

   **Example**

   `volume show -junction -volume data1`
3. Determine the full path to the audited object by appending the relative path found in the `<ObjectName>` tag to the junction path for the volume:

Example

```
/data/data1/dir1/file.txt
```

### Considerations when auditing symlinks and hard links

There are certain considerations you must keep in mind when auditing symlinks and hard links.

An audit record contains information about the object being audited including the path to the audited object, which is identified in the `<ObjectName>` tag. You should be aware of how paths for symlinks and hard links are recorded in the `<ObjectName>` tag.

#### Symlinks

A symlink is a file with a separate inode that contains a pointer to the location of a destination object, known as the target. When accessing an object through a symlink, clustered Data ONTAP automatically interprets the symlink and follows the actual canonical protocol agnostic path to the target object in the volume.

In the following example output, there are two symlinks, both pointing to a file named `target.txt`. One of the symlinks is a relative symlink and one is an absolute symlink. If either of the symlinks are audited, the `<ObjectName>` tag in the audit event contains the path to the file `target.txt`:

```
[root@host1 audit]# ls -l
 total 0
lrwxrwxrwx 1 user1 group1 37 Apr 2 10:09 softlink_fullpath.txt -> /data/audit/target.txt
lrwxrwxrwx 1 user1 group1 10 Apr 2 09:54 softlink.txt -> target.txt
-rwxrwxrwx 1 user1 group1 16 Apr 2 10:05 target.txt
```

#### Hard links

A hard link is a directory entry that associates a name with an existing file on a file system. The hard link points to the inode location of the original file. Similar to how clustered Data ONTAP interprets symlinks, clustered Data ONTAP interprets the hard link and follows the actual canonical path to the target object in the volume. When access to a hard link object is audited, the audit event records this absolute canonical path in the `<ObjectName>` tag rather than the hard link path.

### Considerations when auditing alternate NTFS data streams

There are certain considerations you must keep in mind when auditing files with NTFS alternate data streams.

The location of an object being audited is recorded in an event record using two tags, the `<ObjectName>` tag (the path) and the `<HandleID>` tag (the handle). To properly identify which stream requests are being logged, you must be aware of what clustered Data ONTAP records in these fields for NTFS alternate data streams:

- **EVTX ID**: 4656 events (open and create audit events)
  - The path of the alternate data stream is recorded in the `<ObjectName>` tag.
The handle of the alternate data stream is recorded in the HandleID tag.

• EVTX ID: 4663 events (all other audit events, such as read, write, getattr, and so on)
  • The path of the base file, not the alternate data stream, is recorded in the ObjectName tag.
  • The handle of the alternate data stream is recorded in the HandleID tag.

Example
The following example illustrates how to identify EVTX ID: 4663 events for alternate data streams using the HandleID tag. Even though the ObjectName tag (path) recorded in the read audit event is to the base file path, the HandleID tag can be used to identify the event as an audit record for the alternate data stream.

Stream file names take the form base_file_name:stream_name. In this example, the dir1 directory contains a base file with an alternate data stream having the following paths:

```
/dir1/file1.txt
/dir1/file1.txt:stream1
```

Note: The output in the following event example is truncated as indicated; the output does not display all of the available output tags for the events.

For an EVTX ID 4656 (open audit event), the audit record output for the alternate data stream records the alternate data stream name in the ObjectName tag:

```
- <Event>
  - <System>
    <Provider Name="Netapp-Security-Auditing" />
    <EventID>4656</EventID>
    <EventName>Open Object</EventName>
    [...]
  </System>
  - <EventData>
    [...]
    <Data Name="ObjectType">Stream</Data>
    <Data Name="HandleID">00000000000401;00;000001e4;00176767</Data>
    <Data Name="ObjectName">(data1);/dir1/file1.txt:stream1</Data>
    [...]
  </EventData>
- <Event>
```

For an EVTX ID 4663 (read audit event), the audit record output for the same alternate data stream records the base file name in the ObjectName tag; however, the handle in the HandleID tag is the alternative data stream’s handle and can be used to correlate this event with the alternative data stream:

```
- <Event>
  - <System>
    <Provider Name="Netapp-Security-Auditing" />
    <EventID>4663</EventID>
    <EventName>Read Object</EventName>
    [...]
  </System>
  - <EventData>
    [...]
    <Data Name="ObjectType">Stream</Data>
    <Data Name="HandleID">00000000000401;00;000001e4;00176767</Data>
    <Data Name="ObjectName">/dir1/file1.txt:stream1</Data>
    [...]
  </EventData>
- <Event>
```
NFS file and directory access events that can be audited

Data ONTAP can audit certain NFS file and directory access events. Knowing what access events can be audited is helpful when interpreting results from the converted audit event logs.

You can audit the following NFS file and directory access events:

- READ
- OPEN
- CLOSE
- READDIR
- WRITE
- SETATTR
- CREATE
- LINK
- OPENATTR
- REMOVE
- GETATTR
- VERIFY
- NVERIFY
- RENAME

To reliably audit NFS RENAME events, you should set audit ACEs on directories instead of files because file permissions are not checked for a RENAME operation if the directory permissions are sufficient.

Related tasks

- Configuring auditing for UNIX security style files and directories on page 443
- Determining what the complete path to the audited object is on page 428

Planning the auditing configuration

Before you configure auditing on Storage Virtual Machines (SVMs) with FlexVol volumes, you must understand which configuration options are available and plan the values that you want to set for each option. This information can help you configure the auditing configuration that meets your business needs.

There are certain configuration parameters that are common to all auditing configurations.

Additionally, there are certain parameters that you can use to specify which of two methods are used when rotating the consolidated and converted audit logs. You can specify one of the two following methods when you configure auditing:
• Rotate logs based on log size
  This is the default method used to rotate logs.

• Rotate logs based on a schedule

**Parameters common to all auditing configurations**

There are two required parameters that you must specify when you create the auditing configuration. There are also three optional parameters that you can specify:

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Option</th>
<th>Required</th>
<th>Include</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SVM name</strong></td>
<td><code>-vserver vserver_name</code></td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Name of the SVM on which to create the auditing configuration. The SVM must already exist.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Log destination path</strong></td>
<td><code>-destination text</code></td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Specifies where the converted audit logs are stored. The path must already exist on the SVM. The path can be up to 864 characters in length and must have read-write permissions. If the path is not valid, the audit configuration command fails. If the SVM is an SVM disaster recovery source, the log destination path cannot be on the root volume. This is because root volume content is not replicated to the disaster recovery destination.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type of information</td>
<td>Option</td>
<td>Required</td>
<td>Include</td>
<td>Your values</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------</td>
<td>----------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Categories of events to audit</strong></td>
<td>-events {file-ops</td>
<td>cifs-logon-logoff</td>
<td>cap-staging}</td>
<td>No</td>
</tr>
<tr>
<td>Specifies the categories of events to audit. The following event categories can be audited:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• File access events (both SMB and NFSv4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• CIFS logon and logoff events</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Central access policy staging</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>events</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Central access policy staging events</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Central access policy staging events are a new advanced auditing event available starting with Windows 2012 Active Directory domains. Central access policy staging events log information about changes to central access policies configured in Active Directory.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The default is to audit file access and CIFS logon and logoff events.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> Before you can specify <strong>cap-staging</strong> as an event category, a CIFS server must exist on the SVM.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Although you can enable central access policy staging in the auditing configuration without enabling Dynamic Access Control on the CIFS server, central access policy staging events are generated only if Dynamic Access Control is enabled. Dynamic Access Control is enabled through a CIFS server option. It is not enabled by default.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Log file output format</strong></td>
<td>-format {xml</td>
<td>evtx}</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Determines the output format of the audit logs. The output format can be either Data ONTAP-specific XML or Microsoft Windows EVTX log format. By default, the output format is EVTX.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Log files rotation limit
Determines how many audit log files to retain before rotating the oldest log file out. For example, if you enter a value of 5, the last five log files are retained.
A value of 0 indicates that all the log files are retained. The default value is 0.

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Option</th>
<th>Required</th>
<th>Include</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log files rotation limit</td>
<td>-rotate-limit integer</td>
<td>No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Parameters used for determining when to rotate audit event logs

Rotate logs based on log size
The default is to rotate audit logs based on size. The default log size is 100 MB. If you want to use the default log rotation method and the default log size, you do not need to configure any specific parameters for log rotation. If you do not want to use the default log size, you can configure the -rotate-size parameter to specify a custom log size:

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Option</th>
<th>Required</th>
<th>Include</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log file size limit</td>
<td>-rotate-size {integer{KB}</td>
<td>MB}</td>
<td>GB}</td>
<td>TB}</td>
</tr>
</tbody>
</table>

Rotate logs based on a schedule
If you choose to rotate the audit logs based on a schedule, you can schedule log rotation by using the time-based rotation parameters in any combination.

- If you configure time-based log rotation parameters, logs are rotated based on the configured schedule instead of log size.
- If you use time-based rotation, the -rotate-schedule-minute parameter is mandatory.
- All other time-based rotation parameters are optional.
- The rotation schedule is calculated by using all the time-related values.
  For example, if you specify only the -rotate-schedule-minute parameter, the audit log files are rotated based on the minutes specified on all days of the week, during all hours on all months of the year.
- If you specify only one or two time-based rotation parameters (for example, -rotate-schedule-month and -rotate-schedule-minutes), the log files are rotated based on the minute values that you specified on all days of the week, during all hours, but only during the specified months.
  For example, you can specify that the audit log is to be rotated during the months January, March, and August on all Mondays, Wednesdays, and Saturdays at 10:30 a.m.
- If you specify values for both -rotate-schedule-dayofweek and -rotate-schedule-day, they are considered independently.
  For example, if you specify -rotate-schedule-dayofweek as Friday and -rotate-schedule-day as 13, then the audit logs would be rotated on every Friday and on the 13th day of the specified month, not just on every Friday the 13th.
You can use the following list of available auditing parameters to determine what values to use for configuring a schedule for audit event log rotations:

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Option</th>
<th>Required</th>
<th>Include</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log rotation schedule: Month</td>
<td>-rotate-schedule-month  chron_month</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Determines the monthly schedule for</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rotating audit logs.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Valid values are January through</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>December, and all.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>For example, you can specify that</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>the audit log is to be rotated</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>during the months January, March,</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>and August.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log rotation schedule: Day of week</td>
<td>-rotate-schedule-dayofweek  chron_dayofweek</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Determines the daily (day of week)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>schedule for rotating audit logs.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Valid values are January through</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>December, and all.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>For example, you can specify that</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>the audit log is to be rotated on</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tuesdays and Fridays, or during all</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>the days of a week.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log rotation schedule: Day</td>
<td>-rotate-schedule-day  chron_dayofmonth</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Determines the day of the month</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>schedule for rotating the audit log.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Valid values range from 1 through 31</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>For example, you can specify that</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>the audit log is to be rotated on</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>the 10th and 20th days of a month,</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>or all days of a month.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log rotation schedule: Hour</td>
<td>-rotate-schedule-hour  chron_hour</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Determines the hourly schedule for</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rotating the audit log.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Valid values range from 0 (midnight)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>to 23 (11:00 p.m.). Specifying all</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rotates the audit logs every hour.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>For example, you can specify that</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>the audit log is to be rotated at</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6 (6 a.m.) and 18 (6 p.m.).</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log rotation schedule: Minute</td>
<td>-rotate-schedule-minute  chron_minute</td>
<td>Yes, if</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Determines the minute schedule for</td>
<td></td>
<td>configuring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rotating the audit log.</td>
<td></td>
<td>schedule-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Valid values range from 0 to 59.</td>
<td></td>
<td>based log</td>
<td></td>
<td></td>
</tr>
<tr>
<td>For example, you can specify that</td>
<td></td>
<td>rotation;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>the audit log is to be rotated at</td>
<td></td>
<td>otherwise,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>the 30th minute.</td>
<td></td>
<td>no.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Related concepts

- Configuring file and folder audit policies on page 439
- Auditing requirements and considerations on page 424
- What the supported audit event log formats are on page 425
Creating a file and directory auditing configuration on SVMs

Creating a file and directory auditing configuration on your Storage Virtual Machine (SVM) with FlexVol volumes includes understanding the available configuration options, planning the configuration, and then configuring and enabling the configuration. You can then display information about the auditing configuration to confirm that the resultant configuration is the desired configuration.

Steps

1. Creating the auditing configuration on page 436
   Before you can begin auditing file and directory events, you must create an auditing configuration on the Storage Virtual Machine (SVM).

2. Enabling auditing on the SVM on page 438
   After you finish setting up the auditing configuration, you must enable auditing on the Storage Virtual Machine (SVM).

3. Verifying the auditing configuration on page 438
   After completing the auditing configuration, you should verify that auditing is configured properly and is enabled.

Related concepts

Planning the auditing configuration on page 431
How to configure NTFS audit policies using the Data ONTAP CLI on page 442
Managing auditing configurations on page 447
Securing file access by using Dynamic Access Control (DAC) on page 196

Related tasks

Configuring NTFS audit policies using the Windows Security tab on page 439
Configuring auditing for UNIX security style files and directories on page 443
Enabling and disabling auditing on SVMs on page 447
Deleting an auditing configuration on page 450
Manually rotating the audit event logs on page 447

Creating the auditing configuration

Before you can begin auditing file and directory events, you must create an auditing configuration on the Storage Virtual Machine (SVM).

Before you begin

If you plan on creating an auditing configuration for central access policy staging, a CIFS server must exist on the SVM.

Note: Although you can enable central access policy staging in the auditing configuration without enabling Dynamic Access Control on the CIFS server, central access policy staging events are generated only if Dynamic Access Control is enabled. Dynamic Access Control is enabled through a CIFS server option. It is not enabled by default.
About this task
If the SVM is an SVM disaster recovery source, the destination path cannot be on the root volume.

Step
1. Using the information in the planning worksheet, create the auditing configuration to rotate audit logs based on log size or a schedule:

<table>
<thead>
<tr>
<th>If you want to rotate audit logs by...</th>
<th>Enter...</th>
</tr>
</thead>
</table>
| Log size                             | vserver audit create -vserver vserver_name -destination path -events 
{(file-ops|cifs-logon-logoff|cap-staging)} [-format {xml|evtx}] [-
rotate-limit integer] [-rotate-size {integer[KB|MB|GB|TB|PB]}] |
| A schedule                           | vserver audit create -vserver vserver_name -destination path -events 
{(file-ops|cifs-logon-logoff|cap-staging)} [-format {xml|evtx}] [-

Note: The -rotate-schedule-minute parameter is required if configuring time-based audit log rotation.

Examples
The following example creates an auditing configuration that audits file operations and CIFS logon and logoff events (the default) using size-based rotation. The log format is EVTX (the default). The logs are stored in the /audit_log directory. The log file size limit is 200 MB. The logs are rotated when they reach 200 MB in size:

```
cluster1::> vserver audit create -vserver vsl -destination /audit_log -rotate-size 200MB
```

The following example creates an auditing configuration that audits file operations and CIFS logon and logoff events (the default) using size-based rotation. The log format is EVTX (the default). The log file size limit is 100 MB (the default), and the log rotation limit is 5:

```
cluster1::> vserver audit create -vserver vsl -destination /audit_log -rotate-limit 5
```

The following example creates an auditing configuration that audits file operations, CIFS logon and logoff events, and central access policy staging events using time-based rotation. The log format is EVTX (the default). The audit logs are rotated monthly, at 12:30 p.m. on all days of the week. The log rotation limit is 5:

```
cluster1::> vserver audit create -vserver vsl -destination /audit_log -events file-ops,cifs-logon-logoff,cap-staging -rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour 12 -rotate-schedule-minute 30 -rotate-limit 5
```
Enabling auditing on the SVM

After you finish setting up the auditing configuration, you must enable auditing on the Storage Virtual Machine (SVM).

Before you begin

The SVM audit configuration must already exist.

About this task

When an SVM disaster recovery ID discard configuration is first started (after the SnapMirror initialization is complete) and the SVM has an auditing configuration, clustered Data ONTAP automatically disables the auditing configuration. Auditing is disabled on the read-only SVM to prevent the staging volumes from filling up. You can enable auditing only after the SnapMirror relationship is broken and the SVM is read-write.

Step

1. Enable auditing on the SVM:

   ```bash
   vserver audit enable -vserver vserver_name
   ```

   Example

   ```bash
   vserver audit enable -vserver vs1
   ```

Verifying the auditing configuration

After completing the auditing configuration, you should verify that auditing is configured properly and is enabled.

Step

1. Verify the auditing configuration:

   ```bash
   vserver audit show -instance -vserver vserver_name
   ```

   Example

   The following command displays in list form all auditing configuration information for Storage Virtual Machine (SVM) vs1:

   ```bash
   vserver audit show -instance -vserver vs1
   ```

   ```bash
   Vserver: vs1
   Auditing state: true
   Log Destination Path: /audit_log
   Categories of Events to Audit: file-ops
   Log Format: evtx
   Log File Size Limit: 200MB
   Log Rotation Schedule: Month: -
   Log Rotation Schedule: Day of Week: -
   Log Rotation Schedule: Day: -
   Log Rotation Schedule: Hour: -
   Log Rotation Schedule: Minute: -
   Log Rotation Schedules: -
   Log Files Rotation Limit: 0
   ```
Configuring file and folder audit policies

Implementing auditing on file and folder access events is a two-step process. First you must create and enable an auditing configuration on Storage Virtual Machines (SVMs) with FlexVol volumes. Second, you must configure audit policies on the files and folders that you want to monitor. You can configure audit policies to monitor both successful and failed access attempts.

You can configure both SMB and NFS audit policies. SMB and NFS audit policies have different configuration requirements and audit capabilities.

If the appropriate audit policies are configured, Data ONTAP monitors SMB and NFS access events as specified in the audit policies only if the SMB or NFS servers are running.

Related concepts

- How the Data ONTAP auditing process works on page 422
- SMB events that can be audited on page 426
- Displaying information about audit policies applied to files and directories on page 443
- Securing file access by using Storage-Level Access Guard on page 152

Configuring audit policies on NTFS security-style files and directories

Before you can audit file and directory operations, you must configure audit policies on the files and directories for which you want to collect audit information. This is in addition to setting up and enabling the audit configuration. You can configure NTFS audit policies by using the Windows Security tab or by using the Data ONTAP CLI.

Configuring NTFS audit policies using the Windows Security tab

You can configure audit policies on files and directories by using the Windows Security tab in the Windows Properties window. This is the same method used when configuring audit polices on data residing on a Windows client, which enables customers to use the same GUI interface that they are accustomed to using.

Before you begin

Auditing must be configured on the Storage Virtual Machine (SVM) that contains the data to which you are applying SACLs.

About this task

Configuring NTFS audit policies is done by adding entries to NTFS system access control lists (SACLs) that are associated with an NTFS security descriptor. The security descriptor is then applied to NTFS files and directories. These tasks are automatically handled by the Windows GUI. The security descriptor can contain discretionary access control lists (DACLs) for applying file and folder access permissions, system access control lists (SACLs) for file and folder auditing, or both SACLs and DACLs.

You can set NTFS audit policies for auditing access on individual files and folders using the Windows Security tab in the Windows Properties window by completing the following steps on a Windows host:

Steps

1. From the Tools menu in Windows Explorer, select Map network drive.
2. Complete the Map Network Drive box:
a. Select a **Drive** letter.

b. In the **Folder** box, type the CIFS server name that contains the share holding the data you would like to audit and the name of the share.

**Example**

If your CIFS server name is “CIFS_SERVER” and your share is named “share1”, you should enter `\CIFS_SERVER\share1`.

**Note:** You can specify the IP address of the data interface for the CIFS server instead of the CIFS server name.

c. Click **Finish**.

The drive you selected is mounted and ready with the Windows Explorer window displaying files and folders contained within the share.

3. Select the file or directory for which you want to enable auditing access.

4. Right-click on the file or directory, and select **Properties**.

5. Select the **Security** tab.

6. Click **Advanced**.

7. Select the **Auditing** tab.

8. Perform the desired actions:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Do the following</th>
</tr>
</thead>
</table>
| **Set up auditing for a new user or group** | a. Click Add.  
b. In the **Enter the object name to select** box, type the name of the user or group that you want to add.  
c. Click OK. |
| **Remove auditing from a user or group** | a. In the **Enter the object name to select** box, select the user or group that you want to remove.  
b. Click Remove.  
c. Click OK.  
d. Skip the rest of this procedure. |
| **Change auditing for a user or group** | a. In the **Enter the object name to select** box, select the user or group that you want to change.  
b. Click Edit.  
c. Click OK. |

If you are setting up auditing on a user or group or changing auditing on an existing user or group, the Auditing Entry for `<object>` box opens.

9. In the **Apply to** box, select how you want to apply this auditing entry.

You can select one of the following:

- **This folder, subfolders and files**
• This folder and subfolders
• This folder only
• This folder and files
• Subfolders and files only
• Subfolders only
• Files only

If you are setting up auditing on a single file, the Apply to box is not active. The Apply to defaults to This object only.

Note: Since auditing takes SVM resources, select only the minimal level that provides the auditing events that meet your security requirements.

10. In the Access box, select what you want audited and whether you want to audit successful events, failure events or both.

• To audit successful events, select the Success box.
• To audit failure events, select the Failure box.

You can audit the following events:

• Full control
• Traverse folder / execute file
• List folder / read data
• Read attributes
• Read extended attributes
• Create files / write data
• Create folders / append data
• Write attributes
• Write extended attributes
• Delete subfolders and files
• Delete
• Read permissions
• Change permissions
• Take ownership

Note: Select only the actions that you need to monitor to meet your security requirements. For more information on these auditable events, see your Windows documentation.

11. If you do not want the auditing setting to propagate to subsequent files and folders of the original container, select Apply these auditing entries to objects and/or containers within this container only box.

12. Click Apply.

13. After you finish adding, removing, or editing auditing entries, click OK.
14. In the Auditing box, select the inheritance settings for this folder.

You can choose one of the following:

- Select the Include inheritable auditing entries from this object's parent box.
- Select the Replace all existing inheritable auditing entries on all descendants with inheritable auditing entries from this object box.
- Select both boxes.
- Select neither box.

If you are setting SACLs on a single file, the Replace all existing inheritable auditing entries on all descendants with inheritable auditing entries from this object box is not present in the Auditing dialog box.

Note: Select only the minimal level that provides the auditing events that meet your security requirements.

15. Click OK.

The Auditing box closes.

Related concepts

- SMB events that can be audited on page 426

Related tasks

- Configuring and applying audit policies on NTFS files and folders using the CLI on page 268
- Displaying information about NTFS audit policies on FlexVol volumes using the CLI on page 445
- Displaying information about audit policies using the Windows Security tab on page 443

How to configure NTFS audit policies using the Data ONTAP CLI

You can configure audit policies on files and folders using the Data ONTAP CLI. This enables you to configure NTFS audit policies without needing to connect to the data using an SMB share on a Windows client.

You can configure NTFS audit policies by using the vserver security file-directory command family.

You can only configure NTFS SACLs using the CLI. Configuring NFSv4 SACLs is not supported with this Data ONTAP command family. See the man pages for more information about using these commands to configure and add NTFS SACLs to files and folders.

Related concepts

- Securing file access by using Storage-Level Access Guard on page 152
- SMB events that can be audited on page 426

Related tasks

- Configuring and applying audit policies on NTFS files and folders using the CLI on page 268
- Displaying information about NTFS audit policies on FlexVol volumes using the CLI on page 445

Related information

- Clustered Data ONTAP 8.3.1 man page: vserver security file-directory show - Display file/folder security information
Configuring auditing for UNIX security style files and directories

You configure auditing for UNIX security style files and directories by adding audit ACEs to NFSv4.x ACLs. This allows you to monitor certain NFS file and directory access events for security purposes.

About this task

For NFSv4.x, both discretionary and system ACEs are stored in the same ACL. They are not stored in separate DACLs and SACLs. Therefore, you must exercise caution when adding audit ACEs to an existing ACL to avoid overwriting and losing an existing ACL. The order in which you add the audit ACEs to an existing ACL does not matter.

Steps

1. Retrieve the existing ACL for the file or directory by using the `nfs4_getfacl` or equivalent command.
   For more information about manipulating ACLs, see the man pages of your NFS client.
2. Append the desired audit ACEs.
3. Apply the updated ACL to the file or directory by using the `nfs4_setfacl` or equivalent command.

Related tasks

- Displaying information about NFSv4 audit policies on FlexVol volumes using the CLI on page 250

Related references

- NFS file and directory access events that can be audited on page 431

Related information

- Clustered Data ONTAP 8.3.1 man page: `vserver security file-directory show` - Display file/folder security information

Displaying information about audit policies applied to files and directories

Displaying information about audit policies applied to files and directories enables you to verify that you have the appropriate system access control lists (SACLs) set on specified files and folders.

Related concepts

- Configuring file and folder audit policies on page 439

Displaying information about audit policies using the Windows Security tab

You can display information about audit policies that have been applied to files and directories by using the Security tab in the Windows Properties window. This is the same method used for data
residing on a Windows server, which enables customers to use the same GUI interface that they are accustomed to using.

**About this task**

To display information about SACLs that have been applied to NTFS files and folders, complete the following steps on a Windows host.

**Steps**

1. From the **Tools** menu in Windows Explorer, select **Map network drive**.
2. Complete the **Map Network Drive** dialog box:
   a. Select a **Drive** letter.
   b. In the **Folder** box, type the IP address or CIFS server name of the Storage Virtual Machine (SVM) containing the share that holds both the data you would like to audit and the name of the share.

   **Example**
   If your CIFS server name is “CIFS_SERVER” and your share is named “share1”, you should enter `\CIFS_SERVER\share1`.

   **Note:** You can specify the IP address of the data interface for the CIFS server instead of the CIFS server name.
   c. Click **Finish**.

   The drive you selected is mounted and ready with the Windows Explorer window displaying files and folders contained within the share.
3. Select the file or directory for which you display auditing information.
4. Right-click on the file or directory, and select **Properties**.
5. Select the **Security** tab.
6. Click **Advanced**.
7. Select the **Auditing** tab.
8. Click **Continue**.

   The Auditing box opens. The **Auditing entries** box displays a summary of users and groups that have SACLs applied to them.
9. In the **Auditing entries** box select the user or group whose SACL entries you want displayed.
10. Click **Edit**.

    The Auditing entry for `<object>` box opens.
11. In the **Access** box, view the current SACLs that are applied to the selected object.
12. Click **Cancel** to close the **Auditing entry for <object>** box.
13. Click **Cancel** to close the **Auditing** box.
Displaying information about NTFS audit policies on FlexVol volumes using the CLI

You can display information about NTFS audit policies on FlexVol volumes, including what the security styles and effective security styles are, what permissions are applied, and information about system access control lists. You can use the results to validate your security configuration or to troubleshoot auditing issues.

About this task

You must supply the name of the Storage Virtual Machine (SVM) and the path to the files or folders whose audit information you want to display. You can display the output in summary form or as a detailed list.

- NTFS security-style volumes and qtrees use only NTFS SACLs (system access control lists) for audit policies.
- Files and folders in a mixed security-style volume with NTFS effective security can have NTFS audit policies applied to them.
- Mixed security-style volumes and qtrees can contain some files and directories that use UNIX file permissions, either mode bits or NFSv4 ACLs, and some files and directories that use NTFS file permissions.
- The top level of a mixed security-style volume can have either UNIX or NTFS effective security and might or might not contain NTFS SACLs.
- Because Storage-Level Access Guard security can be configured on a mixed security-style volume or qtree even if the effective security style of the volume root or qtree is UNIX, output for a volume or qtree path where Storage-Level Access Guard is configured might display both regular file and folder NFSv4 SACLs and Storage-Level Access Guard NTFS SACLs.
- If the path entered in the command is to data with NTFS effective security, the output also displays information about Dynamic Access Control ACEs if Dynamic Access Control is configured for the given file or directory path.
- When displaying security information about files and folders with NTFS effective security, UNIX-related output fields contain display-only UNIX file permission information.
- NTFS security-style files and folders use only NTFS file permissions and Windows users and groups when determining file access rights.
- ACL output is displayed only for file and folders with NTFS or NFSv4 security. This field is empty for files and folders using UNIX security that have only mode bit permissions applied (no NFSv4 ACLs).
- The owner and group output fields in the ACL output apply only in the case of NTFS security descriptors.

Step

1. Display file and directory audit policy settings with the desired level of detail:

<table>
<thead>
<tr>
<th>If you want to display information...</th>
<th>Enter the following command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>In summary form</td>
<td><code>vserver security file-directory show -vserver vserver_name -path path</code></td>
</tr>
<tr>
<td>With expanded detail</td>
<td><code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code></td>
</tr>
</tbody>
</table>
Examples

The following example displays the audit policy information about the path /corp in SVM vs1. The path has NTFS effective security. The NTFS security descriptor contains both a SUCCESS and a SUCCESS/FAIL SACL entry.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
Vserver: vs1
File Path: /corp
File Inode Number: 357
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
Unix User Id: 0
Unix Group Id: 0
Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
Control:0x8014
Owner:DOMAIN\Administrator
Group:BUILTIN\Administrators
SACL - ACEs
  ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
  SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
DACL - ACEs
  ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
  ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
  ALLOW-OWNER-0x1f01ff-OI|CI
  ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

The following example displays the audit policy information about the path /datavol1 in SVM vs1. The path contains both regular file and folder SACLs and Storage-Level Access Guard SACLs.

```
cluster::> vserver security file-directory show -vserver vs1 -path /datavol1
Vserver: vs1
File Path: /datavol1
File Inode Number: 77
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
Unix User Id: 0
Unix Group Id: 0
Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
Control:0xa814
Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
SACL - ACEs
  AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|SA|FA
DACL - ACEs
  ALLOW-EXAMPLE\marketing-0x120089-FA
  ALLOW-EXAMPLE\engineering-0x1f01ff-SA
Storage-Level Access Guard security
SACL (Applies to Directories):
  AUDIT-EXAMPLE\Domain Users-0x120089-FA
  AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Directories):
  ALLOW-EXAMPLE\Domain Users-0x120089
  ALLOW-EXAMPLE\engineering-0x1f01ff
SACL (Applies to Files):
  AUDIT-EXAMPLE\Domain Users-0x120089-FA
  AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Files):
  ALLOW-EXAMPLE\Domain Users-0x120089
  ALLOW-EXAMPLE\engineering-0x1f01ff
```

446 | File Access Management Guide for CIFS
Managing auditing configurations

You can manage Storage Virtual Machine (SVM) auditing configurations by manually rotating the audit logs, enabling or disabling auditing, displaying information about auditing configurations, modifying auditing configurations, and deleting auditing configurations. You also need to understand what happens when reverting to a release where auditing is not supported.

Related concepts

Troubleshooting auditing and staging volume space issues on page 451

Manually rotating the audit event logs

Before you can view the audit event logs, the logs must be converted to user-readable formats. If you want to view the event logs for a specific Storage Virtual Machine (SVM) before Data ONTAP automatically rotates the log, you can manually rotate the audit event logs on an SVM.

Step

1. Rotate the audit event logs by using the vserver audit rotate-log command.

   Example

   vserver audit rotate-log -vserver vs1

   The audit event log is saved in the SVM audit event log directory with the format specified by the auditing configuration (XML or EVTX), and can be viewed by using the appropriate application.

Related concepts

Viewing audit event logs on page 425

Related tasks

Creating a file and directory auditing configuration on SVMs on page 436

Enabling and disabling auditing on SVMs

You can enable or disable auditing on Storage Virtual Machines (SVMs). You might want to temporarily stop file and directory auditing by disabling auditing. You can enable auditing at any time (if an auditing configuration exists).

Before you begin

Before you can enable auditing on the SVM, the SVM's auditing configuration must already exist.

About this task

Disabling auditing does not delete the auditing configuration.

Steps

1. Perform the appropriate command:

<table>
<thead>
<tr>
<th>If you want auditing to be...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>vserver audit enable -vserver vserver_name</td>
</tr>
</tbody>
</table>
If you want auditing to be...

<table>
<thead>
<tr>
<th>Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>vserver audit disable -vserver vserver_name</strong></td>
</tr>
</tbody>
</table>

2. Verify that auditing is in the desired state:

**vserver audit show -vserver vserver_name**

### Examples

The following example enables auditing for SVM vs1:

```bash
cluster1::> vserver audit enable -vserver vs1
cluster1::> vserver audit show -vserver vs1
Vserver: vs1
Auditing state: true
Log Destination Path: /audit_log
Categories of Events to Audit: file-ops, cifs-logon-logoff
Log Format: evtx
Log File Size Limit: 100MB
Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
Log Rotation Schedule: Day: -
Log Rotation Schedule: Hour: -
Log Rotation Schedule: Minute: -
Rotation Schedules: -
Log Files Rotation Limit: 10
```

The following example disables auditing for SVM vs1:

```bash
cluster1::> vserver audit disable -vserver vs1
Vserver: vs1
Auditing state: false
Log Destination Path: /audit_log
Categories of Events to Audit: file-ops, cifs-logon-logoff
Log Format: evtx
Log File Size Limit: 100MB
Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
Log Rotation Schedule: Day: -
Log Rotation Schedule: Hour: -
Log Rotation Schedule: Minute: -
Rotation Schedules: -
Log Files Rotation Limit: 10
```

### Related tasks

- Deleting an auditing configuration on page 450

### Displaying information about auditing configurations

You can display information about auditing configurations. The information can help you determine whether the configuration is what you want in place for each SVM. The displayed information also enables you to verify whether an auditing configuration is enabled.

### About this task

You can display detailed information about auditing configurations on all SVMs or you can customize what information is displayed in the output by specifying optional parameters. If you do not specify any of the optional parameters, the following is displayed:

- SVM name to which the auditing configuration applies
- The audit state, which can be **true** or **false**
If the audit state is `true`, auditing is enabled. If the audit state is `false`, auditing is disabled.

- The categories of events to audit
- The audit log format
- The target directory where the auditing subsystem stores consolidated and converted audit logs

**Step**

1. Display information about the auditing configuration by using the `vserver audit show` command.

   For more information about using the command, see the man pages.

**Examples**

The following example displays a summary of the auditing configuration for all SVMs:

```
cluster1::> vserver audit show
Vserver     State  Event Types Log Format Target Directory
----------- ------ ----------- ---------- ---------------------
vs1         false  file-ops    evtx       /audit_log
```

The following example displays, in list form, all auditing configuration information for all SVMs:

```
cluster1::> vserver audit show -instance
Vserver: vs1
Auditing state: true
Log Destination Path: /audit_log
Categories of Events to Audit: file-ops
Log Format: evtx
Log File Size Limit: 100MB
Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
Log Rotation Schedule: Hour: -
Log Rotation Schedule: Minute: -
Rotation Schedules: -
Log Files Rotation Limit: 0
```

**Related tasks**

*Creating a file and directory auditing configuration on SVMs* on page 436

**Commands for modifying auditing configurations**

If you want to change an auditing setting, you can modify the current configuration at any time, including modifying the log path destination and log format, modifying the categories of events to audit, how to automatically save log files, and specify the maximum number of log files to save.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify the log destination path</td>
<td><code>vserver audit modify</code> with the <code>-destination</code> parameter</td>
</tr>
</tbody>
</table>
If you want to... | Use this command...
--- | ---
Modify the category of events to audit | \texttt{vserver audit modify} with the \texttt{-events} parameter
Note: To audit central access policy staging events, the Dynamic Access Control (DAC) CIFS server option must be enabled on the Storage Virtual Machine (SVM).
Modify the log format | \texttt{vserver audit modify} with the \texttt{-format} parameter
Enabling automatic saves based on internal log file size | \texttt{vserver audit modify} with the \texttt{-rotate-size} parameter
Enabling automatic saves based on a time interval | \texttt{vserver audit modify} with the \texttt{-rotate-schedule-month, -rotate-schedule-dayofweek, -rotate-schedule-day, -rotate-schedule-hour, and -rotate-schedule-minute} parameters
Specifying the maximum number of saved log files | \texttt{vserver audit modify} with the \texttt{-rotate-limit} parameter

## Deleting an auditing configuration

In you no longer want to audit file and directory events on the Storage Virtual Machine (SVM) and do not want to maintain an auditing configuration on the SVM, you can delete the auditing configuration.

### Steps

1. Disable the auditing configuration:

   \texttt{vserver audit disable \_vserver vserver\_name}

   Example

   \texttt{vserver audit disable \_vserver vs1}

2. Delete the auditing configuration:

   \texttt{vserver audit delete \_vserver vserver\_name}

   Example

   \texttt{vserver audit delete \_vserver vs1}

### Related tasks

*Enabling and disabling auditing on SVMs* on page 447
What the process is when reverting

If you plan to revert the cluster, you should be aware of the revert process Data ONTAP follows when there are auditing-enabled Storage Virtual Machines (SVMs) in the cluster. You must take certain actions before reverting.

Reverting to a version of clustered Data ONTAP that does not support the auditing of CIFS logon and logoff events and central access policy staging events

Support for auditing of CIFS logon and logoff events and for central access policy staging events starts with clustered Data ONTAP 8.3. If you are reverting to a version of clustered Data ONTAP that does not support these event types and you have auditing configurations that monitor these event types, you must change the auditing configuration for those audit-enabled SVMs before reverting. You must modify the configuration so that only file-op events are audited.

Related tasks

- Enabling and disabling auditing on SVMs on page 447
- Deleting an auditing configuration on page 450

Troubleshooting auditing and staging volume space issues

Issues can arise when there is insufficient space on either the staging volumes or on the volume containing the audit event logs. If there is insufficient space, new audit records cannot be created, which prevents clients from accessing data, and access requests fail. You should know how to troubleshoot and resolve these volume space issues.

Related concepts

- Aggregate space considerations when enabling auditing on page 424

How to troubleshoot space issues related to the event log volumes

If volumes containing event log files run out of space, auditing cannot convert log records into log files. This results in client access failures. You need to know how to troubleshoot space issues related to event log volumes.

- Storage Virtual Machine (SVM) and cluster administrators can determine whether there is insufficient volume space by displaying information about volume and aggregate usage and configuration.

- If there is insufficient space in the volumes containing event logs, SVM and cluster administrators can resolve the space issues by either removing some of the event log files or by increasing the size of the volume.

  Note: If the aggregate that contains the event log volume is full, then the size of the aggregate must be increased before you can increase the size of the volume. Only a cluster administrator can increase the size of an aggregate.

- The destination path for the event log files can be changed to a directory on another volume by modifying the auditing configuration.

For more information about viewing information about volumes and increasing volume size, see the Clustered Data ONTAP Logical Storage Management Guide.

For more information about viewing information about aggregates and managing aggregates, see the Clustered Data ONTAP Physical Storage Management Guide.
How to troubleshoot space issues related to the staging volumes (cluster administrators only)

If any of the volumes containing staging files for your Storage Virtual Machine (SVM) runs out of space, auditing cannot write log records into staging files. This results in client access failures. To troubleshoot this issue, you need to determine whether any of the staging volumes used in the SVM are full by displaying information about volume usage.

If the volume containing the consolidated event log files has sufficient space but there are still client access failures due to insufficient space, then the staging volumes might be out of space. The SVM administrator must contact you to determine whether the staging volumes that contain staging files for the SVM have insufficient space. The auditing subsystem generates an EMS event if auditing events cannot be generated due to insufficient space in a staging volume. The following message is displayed: No space left on device. Only you can view information about staging volumes; SVM administrators cannot.

All staging volume names begin with MDV_aud_ followed by the UUID of the aggregate containing that staging volume. The following example shows four system volumes on the admin SVM, which were automatically created when a file services auditing configuration was created for a data SVM in the cluster:

```
cluster1::> volume show -vserver cluster1
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- ----- 
cluster1  MDV_aud_1d0131843d4811e296fc123478563412  aggr0    online     RW          2GB     1.90GB    5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412  root_vs0  online     RW          2GB     1.90GB    5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412  aggr1    online     RW          2GB     1.90GB    5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412  aggr2    online     RW          2GB     1.90GB    5%
4 entries were displayed.
```

If there is insufficient space in the staging volumes, you can resolve the space issues by increasing the size of the volume.

**Note:** If the aggregate that contains the staging volume is full, then the size of the aggregate must be increased before you can increase the size of the volume. Only you can increase the size of an aggregate; SVM administrators cannot.
Using FPolicy for file monitoring and management on SVMs with FlexVol volumes

FPolicy is a file access notification framework that is used to monitor and manage file access events on Storage Virtual Machines (SVMs) with FlexVol volumes.

The framework generates notifications that are sent to either external FPolicy servers or to Data ONTAP. FPolicy supports event notifications for files and directories that are accessed using NFS and SMB.

Note: FPolicy is not supported on SVMs with Infinite Volume.

How FPolicy works

Before you plan and create your FPolicy configuration, you should understand the basics of how FPolicy works.

What the two parts of the FPolicy solution are

There are two parts to an FPolicy solution. The Data ONTAP FPolicy framework manages activities on the cluster and sends notifications to external FPolicy servers. External FPolicy servers process notifications sent by Data ONTAP FPolicy.

The Data ONTAP framework creates and maintains the FPolicy configuration, monitors file events, and sends notifications to external FPolicy servers. Data ONTAP FPolicy provides the infrastructure that allows communication between external FPolicy servers and Storage Virtual Machine (SVM) nodes.

The FPolicy framework connects to external FPolicy servers and sends notifications for certain file system events to the FPolicy servers when these events occur as a result of client access. The external FPolicy servers process the notifications and send responses back to the node. What happens as a result of the notification processing depends on the application and whether the communication between the node and the external servers is asynchronous or synchronous.

Related concepts

Roles that cluster components play with FPolicy implementation on page 454
How FPolicy works with external FPolicy servers on page 455
How FPolicy services work across SVM namespaces on page 458
FPolicy configuration types on page 458
What the steps for setting up an FPolicy configuration are on page 463

What synchronous and asynchronous notifications are

FPolicy sends notifications to external FPolicy servers via the FPolicy interface. The notifications are sent either in synchronous or asynchronous mode. The notification mode determines what Data ONTAP does after sending notifications to FPolicy servers.

Asynchronous notifications

With asynchronous notifications, the node does not wait for a response from the FPolicy server, which enhances overall throughput of the system. This type of notification is suitable for applications where the FPolicy server does not require that any action be taken as a result of notification evaluation. For example, asynchronous notifications are used
when the Storage Virtual Machine (SVM) administrator wants to monitor and audit file access activity.

**Synchronous notifications**

When configured to run in synchronous mode, the FPolicy server must acknowledge every notification before the client operation is allowed to continue. This type of notification is used when an action is required based on the results of notification evaluation. For example, synchronous notifications are used when the SVM administrator wants to either allow or deny requests based on criteria specified on the external FPolicy server.

**Related concepts**

- *How control channels are used for FPolicy communication* on page 455
- *How privileged data access channels are used for synchronous communication* on page 455

**Synchronous and asynchronous applications**

There are many possible uses for FPolicy applications, both asynchronous and synchronous.

Asynchronous applications are ones where the external FPolicy server does not alter access to files or directories or modify data on the Storage Virtual Machine (SVM). For example:

- File access and audit logging
- Storage resource management

Synchronous applications are ones where data access is altered or data is modified by the external FPolicy server. For example:

- Quota management
- File access blocking
- File archiving and hierarchical storage management
- Encryption and decryption services
- Compression and decompression services

You can use the SDK for FPolicy to identify and implement other applications as well.

**Roles that cluster components play with FPolicy implementation**

The cluster, the contained Storage Virtual Machines (SVMs), and data LIFs all play a role in an FPolicy implementation.

**cluster**

The cluster contains the FPolicy management framework and maintains and manages information about all FPolicy configurations in the cluster.

**SVM**

An FPolicy configuration is defined at the SVM level. The scope of the configuration is the SVM, and it only operates on SVM resources. One SVM configuration cannot monitor and send notifications for file access requests that are made for data residing on another SVM.

FPolicy configurations can be defined on the admin SVM. After configurations are defined on the admin SVM, they can be seen and used in all SVMs.

**data LIFs**

Connections to the FPolicy servers are made through data LIFs belonging to the SVM with the FPolicy configuration. The data LIFs used for these connections can fail over in the same manner as data LIFs used for normal client access.
How FPolicy works with external FPolicy servers

After FPolicy is configured and enabled on the Storage Virtual Machine (SVM), FPolicy runs on every node on which the SVM participates. FPolicy is responsible for establishing and maintaining connections with external FPolicy servers (FPolicy servers), for notification processing, and for managing notification messages to and from FPolicy servers.

Additionally, as part of connection management, FPolicy has the following responsibilities:

- Ensures that file notification flows through the correct LIF to the FPolicy server.
- Ensures that when multiple FPolicy servers are associated with a policy, load balancing is done when sending notifications to the FPolicy servers.
- Attempts to reestablish the connection when a connection to an FPolicy server is broken.
- Sends the notifications to FPolicy servers over an authenticated session.
- Manages the passthrough-read data connection established by the FPolicy server for servicing client requests when passthrough-read is enabled.

How control channels are used for FPolicy communication

FPolicy initiates a control channel connection to an external FPolicy server from the data LIFs of each node participating on a Storage Virtual Machine (SVM). FPolicy uses control channels for transmitting file notifications; therefore, an FPolicy server might see multiple control channel connections based on SVM topology.

How privileged data access channels are used for synchronous communication

With synchronous use cases, the FPolicy server accesses data residing on the Storage Virtual Machine (SVM) through a privileged data access path. Access through the privileged path exposes the complete file system to the FPolicy server. It can access data files to collect information, to scan files, read files, or write into files.

Because the external FPolicy server can access the entire file system from the root of the SVM through the privileged data channel, the privileged data channel connection must be secure.

Related concepts

What granting super user credentials for privileged data access means on page 456

How FPolicy connection credentials are used with privileged data access channels

The FPolicy server makes privileged data access connections to cluster nodes by using a specific Windows user credential that is saved with the FPolicy configuration. SMB is the only supported protocol for making a privileged data access channel connection.

If the FPolicy server requires privileged data access, the following conditions must be met:

- A CIFS license must be enabled on the cluster.
- The FPolicy server must run under the credentials configured in the FPolicy configuration.

When making a data channel connection, FPolicy uses the credential for the specified Windows user name. Data access is made over the admin share ONTAP_ADMIN$.
What granting super user credentials for privileged data access means

Data ONTAP uses the combination of the IP address and the user credential configured in the FPolicy configuration to grant super user credentials to the FPolicy server.

Super user status grants the following privileges when the FPolicy server accesses data:

- **Avoid permission checks**
  The user avoids checks on files and directory access.

- **Special locking privileges**
  Data ONTAP allows read, write, or modify access to any file regardless of existing locks. If the FPolicy server takes byte range locks on the file, it results in immediate removal of existing locks on the file.

- **Bypass any FPolicy checks**
  Access does not generate any FPolicy notifications.

How FPolicy manages policy processing

There might be multiple FPolicy policies assigned to your Storage Virtual Machine (SVM); each with a different priority. To create an appropriate FPolicy configuration on the SVM, it is important to understand how FPolicy manages policy processing.

Each file access request is initially evaluated to determine which policies are monitoring this event. If it is a monitored event, information about the monitored event along with interested policies is passed to FPolicy where it is evaluated. Each policy is evaluated in order of the assigned priority.

You should consider the following recommendations when configuring policies:

- **When you want a policy to always be evaluated before other policies, configure that policy with a higher priority.**

- **If the success of requested file access operation on a monitored event is a prerequisite for a file request that is evaluated against another policy, give the policy that controls the success or failure of the first file operation a higher priority.**
  For example, if one policy manages FPolicy file archiving and restore functionality and a second policy manages file access operations on the online file, the policy that manages file restoration must have a higher priority so that the file is restored before the operation managed by the second policy can be allowed.

- **If you want all policies that might apply to a file access operation to be evaluated, give synchronous policies a lower priority.**

You can reorder policy priorities for existing policies by modifying the policy sequence number. However, to have FPolicy evaluate policies based on the modified priority order, you must disable and reenable the policy with the modified sequence number.

Related concepts

*Planning the FPolicy policy configuration* on page 477

What the node-to-external FPolicy server communication process is

To properly plan your FPolicy configuration, you should understand what the node-to-external FPolicy server communication process is.

Every node that participates on each Storage Virtual Machine (SVM) initiates a connection to an external FPolicy server (FPolicy server) using TCP/IP. Connections to the FPolicy servers are set up using node data LIFs; therefore, a participating node can set up a connection only if the node has an operational data LIF for the SVM.
Each FPolicy process on participating nodes attempts to establish a connection with the FPolicy server when the policy is enabled. It uses the IP address and port of the FPolicy external engine specified in the policy configuration.

The connection establishes a control channel from each of the nodes participating on each SVM to the FPolicy server through the data LIF. In addition, if IPv4 and IPv6 data LIF addresses are present on the same participating node, FPolicy attempts to establish connections for both IPv4 and IPv6. Therefore, in a scenario where the SVM extends over multiple nodes or if both IPv4 and IPv6 addresses are present, the FPolicy server must be ready for multiple control channel setup requests from the cluster after the FPolicy policy is enabled on the SVM.

For example, if a cluster has three nodes—Node1, Node2, and Node3—and SVM data LIFs are spread across only Node2 and Node3, control channels are initiated only from Node2 and Node3, irrespective of the distribution of data volumes. Say that Node2 has two data LIFs—LIF1 and LIF2—that belong to the SVM and that the initial connection is from LIF1. If LIF1 fails, FPolicy attempts to establish a control channel from LIF2.

How FPolicy manages external communication during LIF migration or failover

Data LIFs can be migrated to data ports in the same node or to data ports on a remote node.

When a data LIF fails over or is migrated, a new control channel connection is made to the FPolicy server. FPolicy can then retry SMB and NFS client requests that timed out, with the result that new notifications are sent to the external FPolicy servers. The node rejects FPolicy server responses to original, timed-out SMB and NFS requests.

How FPolicy manages external communication during node failover

If the cluster node that hosts the data ports used for FPolicy communication fails, Data ONTAP breaks the connection between the FPolicy server and the node.

The impact of cluster failover to the FPolicy server can be mitigated by configuring the LIF manager to migrate the data port used in FPolicy communication to another active node. After the migration is complete, a new connection is established using the new data port.

If the LIF manager is not configured to migrate the data port, the FPolicy server must wait for the failed node to come up. After the node is up, a new connection is initiated from that node with a new Session ID.
**Note:** The FPolicy server detects broken connections with the keep-alive protocol message. The timeout for purging the session ID is determined when configuring FPolicy. The default keep-alive timeout is two minutes.

**How FPolicy services work across SVM namespaces**

Data ONTAP provides a unified Storage Virtual Machine (SVM) namespace. Volumes across the cluster are joined together by junctions to provide a single, logical file system. The FPolicy server is aware of the namespace topology and provides FPolicy services across the namespace.

The namespace is specific to and contained within the SVM; therefore, you can see the namespace only from the SVM context. Namespaces have the following characteristics:

- A single namespace exists in each SVM, with the root of the namespace being the root volume, represented in the namespace as slash (/).
- All other volumes have junction points below the root (/).
- Volume junctions are transparent to clients.
- A single NFS export can provide access to the complete namespace; otherwise, export policies can export specific volumes.
- SMB shares can be created on the volume or on qtrees within the volume, or on any directory within the namespace.
- The namespace architecture is flexible.

Examples of typical namespace architectures are as follows:

- A namespace with a single branch off of the root
- A namespace with multiple branches off of the root
- A namespace with multiple unbranched volumes off of the root

**Related concepts**

*How namespaces and volume junctions affect SMB access on SVMs with FlexVol volumes* on page 15

*Creating and managing data volumes in NAS namespaces* on page 148

**FPolicy configuration types**

There are two basic FPolicy configuration types. One configuration uses external FPolicy servers to process and act upon notifications. The other configuration does not use external FPolicy servers; instead, it uses the Data ONTAP internal, native FPolicy server for simple file blocking based on extensions.

**External FPolicy server configuration**

The notification is sent to the FPolicy server, which screens the request and applies rules to determine whether the node should allow the requested file operation. For synchronous policies, the FPolicy server then sends a response to the node to either allow or block the requested file operation.

**Native FPolicy server configuration**

The notification is screened internally. The request is allowed or denied based on file extension settings configured in the FPolicy scope.
When to create a native FPolicy configuration

Native FPolicy configurations use the Data ONTAP internal FPolicy engine to monitor and block file operations based on the file's extension. This solution does not require external FPolicy servers (FPolicy servers). Using a native file blocking configuration is appropriate when this simple solution is all that is needed.

Native file blocking enables you to monitor any file operations that match configured operation and filtering events and then deny access to files with particular extensions. This is the default configuration.

This configuration provides a means to block file access based only on the file's extension. For example, to block files that contain .mp3 extensions, you configure a policy to provide notifications for certain operations with target file extensions of .mp3. The policy is configured to deny .mp3 file requests for operations that generate notifications.

The following applies to native FPolicy configurations:

- The same set of filters and protocols that are supported by FPolicy server-based file screening are also supported for native file blocking.

- Native file blocking and FPolicy server-based file screening applications can be configured at the same time.
  
To do so, you can configure two separate FPolicy policies for the Storage Virtual Machine (SVM), with one configured for native file blocking and one configured for FPolicy server-based file screening.

- The native file blocking feature only screens files based on the extensions and not on the content of the file.

- In the case of symbolic links, native file blocking uses the file extension of the root file.

When to create a configuration that uses external FPolicy servers

FPolicy configurations that use external FPolicy servers to process and manage notifications provide robust solutions for use cases where more than simple file blocking based on file extension is needed.

You should create a configuration that uses external FPolicy servers when you want to do such things as monitor and record file access events, provide quota services, perform file blocking based on criteria other than simple file extensions, provide data migration services using hierarchical storage management applications, or provide a fine-grained set of policies that monitor only a subset of data in the Storage Virtual Machine (SVM).

How FPolicy passthrough-read enhances usability for hierarchical storage management

FPolicy passthrough-read enhances usability for hierarchical storage management (HSM). Passthrough-read enables the FPolicy server (functioning as the HSM server) to provide read access to offline files without having to recall the file from the secondary storage system to the primary storage system.

When an FPolicy server is configured to provide HSM to files residing on a CIFS server, policy-based file migration occurs where the files are stored offline on secondary storage and only a stub file
remains on primary storage. Even though a stub file appears as a normal file to clients, it is actually a sparse file that is the same size of the original file. The sparse file has the CIFS offline bit set and points to the actual file that has been migrated to secondary storage.

Typically when a read request for an offline file is received, the requested content must be recalled back to primary storage and then accessed through primary storage. The need to recall data back to primary storage has several undesirable effects. Among the undesirable effects is the increased latency to client requests caused by the need to recall the content before responding to the request and the increased space consumption needed for recalled files on the primary storage.

FPolicy passthrough-read allows the HSM server (the FPolicy server) to provide read access to migrated, offline files without having to recall the file from the secondary storage system to the primary storage system. Instead of recalling the files back to primary storage, read requests can be serviced directly from secondary storage.

Passthrough-read enhances usability by providing the following benefits:

- Read requests can be serviced even if the primary storage does not have sufficient space to recall requested data back to primary storage.
- Better capacity and performance management when a surge of data recall might occur, such as if a script or a backup solution needs to access many offline files.
- Read requests for offline files in Snapshot copies can be serviced. Because Snapshot copies are read-only, the FPolicy server cannot restore the original file if the stub file is located in a Snapshot copy. Using passthrough-read eliminates this problem.
- Policies can be set up that control when read requests are serviced through access to the file on secondary storage and when the offline file should be recalled to primary storage. For example, a policy can be created on the HSM server that specifies the number of times the offline file can be accessed in a specified period of time before the file is migrated back to primary storage. This type of policy avoids recalling files that are rarely accessed.

Related concepts

*Passthrough-read upgrade and revert considerations* on page 462

**How read requests are managed when FPolicy passthrough-read is enabled**

You should understand how read requests are managed when FPolicy passthrough-read is enabled so that you can optimally configure connectivity between the Storage Virtual Machine (SVM) and the FPolicy servers.

When FPolicy passthrough-read is enabled and the SVM receives a request for an offline file, FPolicy sends a notification to the FPolicy server (HSM server) through the standard connection channel.

After receiving the notification, the FPolicy server reads the data from the file path sent in the notification and sends the requested data to the SVM through the passthrough-read privileged data connection that is established between the SVM and the FPolicy server.

After the data is sent, the FPolicy server then responds to the read request as an ALLOW or DENY. Based on whether the read request is allowed or denied, Data ONTAP either sends the requested information or sends an error message to the client.
Requirements, considerations, and best practices for configuring FPolicy

Before you create and configure FPolicy configurations on your Storage Virtual Machines (SVMs) with FlexVol volumes, you need to be aware of certain requirements, considerations, and best practices for configuring FPolicy.

Related concepts

- Passthrough-read upgrade and revert considerations on page 462
- Planning the FPolicy policy configuration on page 477
- Creating the FPolicy configuration on page 485

Ways to configure FPolicy

FPolicy features are configured either through the command line interface (CLI) or through APIs. This guide uses the CLI to create, manage, and monitor an FPolicy configuration on the cluster.

Requirements for setting up FPolicy

Before you configure and enable FPolicy on your Storage Virtual Machine (SVM), you need to be aware of certain requirements.

- All nodes in the cluster must be running a version of Data ONTAP that supports FPolicy.
- If you are not using the Data ONTAP native FPolicy engine, you must have external FPolicy servers (FPolicy servers) installed.
- The FPolicy servers must be installed on a server accessible from the data LIFs of the SVM where FPolicy policies are enabled.
- The IP address of the FPolicy server must be configured as a primary or secondary server in the FPolicy policy external engine configuration.
- If the FPolicy servers access data over a privileged data channel, the following additional requirements must be met:
  - CIFS must be licensed on the cluster. Privileged data access is accomplished using SMB connections.
  - A user credential must be configured for accessing files over the privileged data channel.
  - The FPolicy server must run under the credentials configured in the FPolicy configuration.
  - All data LIFs used to communicate with the FPolicy servers must be configured to have cifs as one of the allowed protocols.
    This includes the LIFs used for passthrough-read connections.

Related concepts

- Planning the FPolicy external engine configuration on page 464
- How privileged data access channels are used for synchronous communication on page 455
- How FPolicy connection credentials are used with privileged data access channels on page 455
- What granting super user credentials for privileged data access means on page 456
Best practices and recommendations when setting up FPolicy

When setting up FPolicy on Storage Virtual Machines (SVMs), you need to be familiar with configuration best practices and recommendations to ensure that your FPolicy configuration provides robust monitoring performance and results that meet your requirements.

- External FPolicy servers (FPolicy servers) should be placed in close proximity to the cluster with high-bandwidth connectivity to provide minimal latency and high-bandwidth connectivity.

- The FPolicy external engine should be configured with more than one FPolicy server to provide resiliency and high availability of FPolicy server notification processing, especially if policies are configured for synchronous screening.

- It is recommended that you disable the FPolicy policy before making any configuration changes. For example, if you want to add or modify an IP address in the FPolicy external engine configured for the enabled policy, you should first disable the policy.

- The cluster node-to-FPolicy server ratio should be optimized to ensure that FPolicy servers are not overloaded, which can introduce latencies when the SVM responds to client requests. The optimal ratio depends on the application for which the FPolicy server is being used.

Related concepts

Planning the FPolicy external engine configuration on page 464

Related tasks

Enabling or disabling FPolicy policies on page 491

Passthrough-read upgrade and revert considerations

There are certain upgrade and revert considerations that you must know about before upgrading to a Data ONTAP release that supports passthrough-read or before reverting to a release that does not support passthrough-read.

Upgrading

After all nodes are upgraded to a version of Data ONTAP that supports FPolicy passthrough-read, the cluster is capable of using the passthrough-read functionality; however, passthrough-read is disabled by default on existing FPolicy configurations. To use passthrough-read on existing FPolicy configurations, you must disable the FPolicy policy and modify the configuration, and then reenable the configuration.

Reverting

Before reverting to a version of Data ONTAP that does not support FPolicy passthrough-read, the following conditions must be met:

- All the policies using passthrough-read must be disabled, and then the affected configurations must be modified so that they do not use passthrough-read.

- FPolicy functionality must be disabled on the cluster by disabling every FPolicy policy on the cluster.
What the steps for setting up an FPolicy configuration are

Before FPolicy can monitor file access, an FPolicy configuration must be created and enabled on the Storage Virtual Machine (SVM) for which FPolicy services are required.

The steps for setting up and enabling an FPolicy configuration on the SVM are as follows:

1. Create an FPolicy external engine.
   The FPolicy external engine identifies the external FPolicy servers (FPolicy servers) that are associated with a specific FPolicy configuration. If the internal “native” FPolicy engine is used to create a native file-blocking configuration, you do not need to create an FPolicy external engine.

2. Create an FPolicy event.
   An FPolicy event describes what the FPolicy policy should monitor. Events consist of the protocols and file operations to monitor, and can contain a list of filters. Events use filters to narrow the list of monitored events for which the FPolicy external engine must send notifications. Events also specify whether the policy monitors volume operations.

3. Create an FPolicy policy.
   The FPolicy policy is responsible for associating, with the appropriate scope, the set of events that need to be monitored and for which of the monitored events notifications must be sent to the designated FPolicy server (or to the native engine if no FPolicy servers are configured). The policy also defines whether the FPolicy server is allowed privileged access to the data for which it receives notifications. An FPolicy server needs privileged access if the server needs to access the data. Typical use cases where privileged access is needed include file blocking, quota management, and hierarchical storage management. The policy is where you specify whether the configuration for this policy uses an FPolicy server or the internal “native” FPolicy server.
   A policy specifies whether screening is mandatory. If screening is mandatory and all FPolicy servers are down or no response is received from the FPolicy servers within a defined timeout period, then file access is denied.
   A policy's boundaries are the SVM. A policy cannot apply to more than one SVM. However, a specific SVM can have multiple FPolicy policies, each with the same or different combination of scope, event, and external server configurations.

4. Configure the policy scope.
   The FPolicy scope determines which volumes, shares, or export-policies the policy acts on or excludes from monitoring. A scope also determines which file extensions should be included or excluded from FPolicy monitoring.

   **Note:** Exclude lists take precedence over include lists.

5. Enable the FPolicy policy.
   When the policy is enabled, the control channels and, optionally, the privileged data channels are connected. The FPolicy process on the nodes on which the SVM participates begin monitoring file and folder access and, for events that match configured criteria, sends notifications to the FPolicy servers (or to the native engine if no FPolicy servers are configured).

   **Note:** If the policy uses native file blocking, an external engine is not configured or associated with the policy.

**Related concepts**

*Planning the FPolicy configuration* on page 464
*Creating the FPolicy configuration* on page 485
Planning the FPolicy configuration

Before you create an FPolicy configuration, you must understand what is involved in each step of the configuration. You need to decide what settings you need to use when performing the configuration and record them in the planning worksheets.

You need to plan for the following configuration tasks:

- Creating the FPolicy external engine
- Creating the FPolicy policy event
- Creating the FPolicy policy
- Creating the FPolicy policy scope

FPolicy is supported on Storage Virtual Machines (SVMs) with FlexVol volumes. FPolicy is not supported on SVMs with Infinite Volume.

Related concepts

- What the steps for setting up an FPolicy configuration are on page 463
- Creating the FPolicy configuration on page 485

Planning the FPolicy external engine configuration

Before you configure the FPolicy external engine (external engine), you must understand what it means to create an external engine and which configuration parameters are available. This information helps you to determine which values to set for each parameter.

Information that is defined when creating the FPolicy external engine

The external engine configuration defines the information that FPolicy needs to make and manage connections to the external FPolicy servers (FPolicy servers), including the following information:

- Storage Virtual Machine (SVM) name
- Engine name
- The IP addresses of the primary and secondary FPolicy servers and the TCP port number to use when making the connection to the FPolicy servers
- Whether the engine type is asynchronous or synchronous
- How to authenticate the connection between the node and the FPolicy server
  If you choose to configure mutual SSL authentication, then you must also configure parameters that provide SSL certificate information.
- How to manage the connection using various advanced privilege settings
  This includes parameters that define such things as timeout values, retry values, keep-alive values, maximum request values, sent and receive buffer size values, and session timeout values.

The `vserver fpolicy policy external-engine create` command is used to create an FPolicy external engine.

What the basic external engine parameters are

You can use the following table of basic FPolicy configuration parameters to help you plan your configuration:
<table>
<thead>
<tr>
<th>Type of information</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SVM</strong></td>
<td>-vserver</td>
</tr>
<tr>
<td>Specifies the SVM name that</td>
<td>vserver_name</td>
</tr>
<tr>
<td>you want to associate with</td>
<td></td>
</tr>
<tr>
<td>this external engine.</td>
<td></td>
</tr>
<tr>
<td>Each FPolicy configuration</td>
<td>-engine-name</td>
</tr>
<tr>
<td>is defined within a single</td>
<td>engine_name</td>
</tr>
<tr>
<td>SVM. The external engine,</td>
<td></td>
</tr>
<tr>
<td>policy event, policy scope,</td>
<td></td>
</tr>
<tr>
<td>and policy that combine</td>
<td></td>
</tr>
<tr>
<td>together to create an</td>
<td></td>
</tr>
<tr>
<td>FPolicy policy configuration</td>
<td></td>
</tr>
<tr>
<td>must all be associated with</td>
<td></td>
</tr>
<tr>
<td>the same SVM.</td>
<td></td>
</tr>
<tr>
<td><strong>Engine name</strong></td>
<td>-primary-servers</td>
</tr>
<tr>
<td>Specifies the name to</td>
<td>IP_address,</td>
</tr>
<tr>
<td>assign to the external</td>
<td></td>
</tr>
<tr>
<td>engine configuration. You</td>
<td></td>
</tr>
<tr>
<td>must specify the external</td>
<td></td>
</tr>
<tr>
<td>engine name later when you</td>
<td></td>
</tr>
<tr>
<td>create the FPolicy policy.</td>
<td></td>
</tr>
<tr>
<td>This associates the external</td>
<td></td>
</tr>
<tr>
<td>engine with the policy.</td>
<td></td>
</tr>
<tr>
<td>The name can be up to 256</td>
<td></td>
</tr>
<tr>
<td>characters long.</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> The name should</td>
<td></td>
</tr>
<tr>
<td>be up to 200 characters</td>
<td></td>
</tr>
<tr>
<td>long if configuring the</td>
<td></td>
</tr>
<tr>
<td>external engine name in a</td>
<td></td>
</tr>
<tr>
<td>MetroCluster or SVM disaster</td>
<td></td>
</tr>
<tr>
<td>recovery configuration.</td>
<td></td>
</tr>
<tr>
<td>The name can contain any</td>
<td></td>
</tr>
<tr>
<td>combination of the following</td>
<td></td>
</tr>
<tr>
<td>ASCII-range characters:</td>
<td></td>
</tr>
<tr>
<td>• a through z</td>
<td></td>
</tr>
<tr>
<td>• A through Z</td>
<td></td>
</tr>
<tr>
<td>• 0 through 9</td>
<td></td>
</tr>
<tr>
<td>• “_”, “-”, and “.”</td>
<td></td>
</tr>
<tr>
<td><strong>Primary FPolicy servers</strong></td>
<td>-port</td>
</tr>
<tr>
<td>Specifies the primary FPolicy</td>
<td>integer</td>
</tr>
<tr>
<td>servers to which the node</td>
<td></td>
</tr>
<tr>
<td>sends notifications for a</td>
<td></td>
</tr>
<tr>
<td>given FPolicy policy. The</td>
<td></td>
</tr>
<tr>
<td>value is specified as a</td>
<td></td>
</tr>
<tr>
<td>comma-delimited list of IP</td>
<td></td>
</tr>
<tr>
<td>addresses.</td>
<td></td>
</tr>
<tr>
<td>If more than one primary</td>
<td></td>
</tr>
<tr>
<td>server IP address is</td>
<td></td>
</tr>
<tr>
<td>specified, every node on</td>
<td></td>
</tr>
<tr>
<td>which the SVM participates</td>
<td></td>
</tr>
<tr>
<td>creates a control connection</td>
<td></td>
</tr>
<tr>
<td>to every specified primary</td>
<td></td>
</tr>
<tr>
<td>FPolicy server at the time</td>
<td></td>
</tr>
<tr>
<td>the policy is enabled.</td>
<td></td>
</tr>
<tr>
<td>If you configure multiple</td>
<td></td>
</tr>
<tr>
<td>primary FPolicy servers,</td>
<td></td>
</tr>
<tr>
<td>notifications are sent to</td>
<td></td>
</tr>
<tr>
<td>the FPolicy servers in a</td>
<td></td>
</tr>
<tr>
<td>round-robin fashion.</td>
<td></td>
</tr>
<tr>
<td>If the external engine is</td>
<td></td>
</tr>
<tr>
<td>used in a MetroCluster or</td>
<td></td>
</tr>
<tr>
<td>SVM disaster recovery</td>
<td></td>
</tr>
<tr>
<td>configuration, you should</td>
<td></td>
</tr>
<tr>
<td>specify the IP addresses of</td>
<td></td>
</tr>
<tr>
<td>the FPolicy servers at the</td>
<td></td>
</tr>
<tr>
<td>source site as primary</td>
<td></td>
</tr>
<tr>
<td>servers. The IP addresses</td>
<td></td>
</tr>
<tr>
<td>of the FPolicy servers at</td>
<td></td>
</tr>
<tr>
<td>the destination site should</td>
<td></td>
</tr>
<tr>
<td>be specified as secondary</td>
<td></td>
</tr>
<tr>
<td>servers.</td>
<td></td>
</tr>
<tr>
<td><strong>Port number</strong></td>
<td></td>
</tr>
<tr>
<td>Specifies the port number</td>
<td></td>
</tr>
<tr>
<td>of the FPolicy service.</td>
<td></td>
</tr>
<tr>
<td>Type of information</td>
<td>Option</td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>-----------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Secondary FPolicy servers</strong></td>
<td>-secondary-server\nservers IP_address,...</td>
</tr>
<tr>
<td>Specifies the secondary FPolicy servers to which to send file access events for a given FPolicy policy. The value is specified as a comma-delimited list of IP addresses. Secondary servers are used only when none of the primary servers are reachable. Connections to secondary servers are established when the policy is enabled, but notifications are sent to secondary servers only if none of the primary servers are reachable. If you configure multiple secondary servers, notifications are sent to the FPolicy servers in a round-robin fashion.</td>
<td></td>
</tr>
<tr>
<td><strong>External engine type</strong></td>
<td>-extern-engine-type\nexternal_engine_type</td>
</tr>
<tr>
<td>Specifies whether the external engine operates in synchronous or asynchronous mode. By default, FPolicy operates in synchronous mode. When set to synchronous, file request processing sends a notification to the FPolicy server, but then does not continue until after receiving a response from the FPolicy server. At that point, request flow either continues or processing results in denial, depending on whether the response from the FPolicy server permits the requested action. When set to asynchronous, file request processing sends a notification to the FPolicy server, and then continues.</td>
<td>The value for this parameter can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• synchronous</td>
</tr>
<tr>
<td></td>
<td>• asynchronous</td>
</tr>
<tr>
<td><strong>SSL option for communication with FPolicy server</strong></td>
<td>-ssl-option [no-auth</td>
</tr>
<tr>
<td>Specifies the SSL option for communication with the FPolicy server. This is a required parameter. You can choose one of the options based on the following information:</td>
<td></td>
</tr>
<tr>
<td>• When set to no-auth, no authentication takes place. The communication link is established over TCP.</td>
<td></td>
</tr>
<tr>
<td>• When set to server-auth, the SVM authenticates the FPolicy server using SSL server authentication.</td>
<td></td>
</tr>
<tr>
<td>• When set to mutual-auth, mutual authentication takes place between the SVM and the FPolicy server; the SVM authenticates the FPolicy server, and the FPolicy server authenticates the SVM. If you choose to configure mutual SSL authentication, then you must also configure the -certificate-common-name, -certificate-serial, and -certificate-ca parameters.</td>
<td></td>
</tr>
<tr>
<td><strong>Certificate FQDN or custom common name</strong></td>
<td>-certificate-common-name text</td>
</tr>
<tr>
<td>Specifies the certificate name used if SSL authentication between the SVM and the FPolicy server is configured. You can specify the certificate name as an FQDN or as a custom common name. If you specify mutual-auth for the -ssl-option parameter, you must specify a value for the -certificate-common-name parameter.</td>
<td></td>
</tr>
<tr>
<td><strong>Certificate serial number</strong></td>
<td>-certificate-serial text</td>
</tr>
<tr>
<td>Specifies the serial number of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured. If you specify mutual-auth for the -ssl-option parameter, you must specify a value for the -certificate-serial parameter.</td>
<td></td>
</tr>
</tbody>
</table>
### Certificate authority

Specifies the CA name of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured.

If you specify `mutual-auth` for the `-ssl-option` parameter, you must specify a value for the `-certificate-ca` parameter.

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate authority</td>
<td><code>-certificate-ca text</code></td>
</tr>
</tbody>
</table>

### What the advanced external engine options are

You can use the following table of advanced FPolicy configuration parameters as you plan whether to customize your configuration with advanced parameters. You use these parameters to modify communication behavior between the cluster nodes and the FPolicy servers:

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout for canceling a request</td>
<td>`-reqs-cancel-timeout integer[h</td>
</tr>
<tr>
<td>Specifies the time interval in hours (h), minutes (m), or seconds (s) that the node waits for a response from the FPolicy server. If the timeout interval passes, the node sends a cancel request to the FPolicy server. The node then sends the notification to an alternate FPolicy server. This timeout helps in handling an FPolicy server that is not responding, which can improve SMB/NFS client response. Also, canceling requests after a timeout period can help in releasing system resources because the notification request is moved from a down/bad FPolicy server to an alternate FPolicy server. The range for this value is 0 through 100. If the value is set to 0, the option is disabled and cancel request messages are not sent to the FPolicy server. The default is 20s.</td>
<td></td>
</tr>
<tr>
<td>Timeout for aborting a request</td>
<td>`-reqs-abort-timeout integer[h</td>
</tr>
<tr>
<td>Specifies the timeout in hours (h), minutes (m), or seconds (s) for aborting a request. The range for this value is 0 through 200.</td>
<td></td>
</tr>
<tr>
<td>Interval for sending status requests</td>
<td>`-status-req-interval integer[h</td>
</tr>
<tr>
<td>Specifies the interval in hours (h), minutes (m), or seconds (s) after which a status request is sent to the FPolicy server. The range for this value is 0 through 50. If the value is set to 0, the option is disabled and status request messages are not sent to the FPolicy server. The default is 10s.</td>
<td></td>
</tr>
<tr>
<td>Maximum outstanding requests on the FPolicy server</td>
<td><code>-max-server-reqs integer</code></td>
</tr>
<tr>
<td>Specifies the maximum number of outstanding requests that can be queued on the FPolicy server. The range for this value is 1 through 10000. The default is 50.</td>
<td></td>
</tr>
<tr>
<td>Type of information</td>
<td>Option</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Timeout for disconnecting a nonresponsive FPolicy server</strong></td>
<td>-server-progress-timeout integer[h</td>
</tr>
<tr>
<td>Specifies the time interval in hours (h), minutes (m), or seconds (s) after which the connection to the FPolicy server is terminated. The connection is terminated after the timeout period only if the FPolicy server's queue contains the maximum allowed requests and no response is received within this timeout period. The maximum allowed number of requests is either 50 (the default) or the number specified by the max-server-reqs-parameter. The range for this value is 1 through 100. The default is 60s.</td>
<td></td>
</tr>
<tr>
<td><strong>Interval for sending keep-alive messages to the FPolicy server</strong></td>
<td>-keep-alive-interval-integer[h</td>
</tr>
<tr>
<td>Specifies the time interval in hours (h), minutes (m), or seconds (s) at which keep-alive messages are sent to the FPolicy server. Keep-alive messages detect half-open connections. The range for this value is 10 through 600. If the value is set to 0, the option is disabled and keep-alive messages are prevented from being sent to the FPolicy servers. The default is 120s.</td>
<td></td>
</tr>
<tr>
<td><strong>Maximum reconnect attempts</strong></td>
<td>-max-connection-retries integer</td>
</tr>
<tr>
<td>Specifies the maximum number of times the SVM attempts to reconnect to the FPolicy server after the connection has been broken. The range for this value is 0 through 20. The default is 5.</td>
<td></td>
</tr>
<tr>
<td><strong>Receive buffer size</strong></td>
<td>-recv-buffer-size integer</td>
</tr>
<tr>
<td>Specifies the receive buffer size of the connected socket for the FPolicy server. The default value is set to 256 kilobytes (Kb). When the value is set to 0, the size of the receive buffer is set to a value defined by the system. For example, if the default receive buffer size of the socket is 65536 bytes, by setting the tunable value to 0, the socket buffer size is set to 65536 bytes. You can use any non-default value to set the size (in bytes) of the receive buffer.</td>
<td></td>
</tr>
<tr>
<td><strong>Send buffer size</strong></td>
<td>-send-buffer-size integer</td>
</tr>
<tr>
<td>Specifies the send buffer size of the connected socket for the FPolicy server. The default value is set to 256 kilobytes (Kb). When the value is set to 0, the size of the send buffer is set to a value defined by the system. For example, if the default send buffer size of the socket is set to 65536 bytes, by setting the tunable value to 0, the socket buffer size is set to 65536 bytes. You can use any non-default value to set the size (in bytes) of the send buffer.</td>
<td></td>
</tr>
<tr>
<td><strong>Timeout for purging a session ID during reconnection</strong></td>
<td>-session-timeout [integer</td>
</tr>
<tr>
<td>Specifies the interval in hours (h), minutes (m), or seconds (s) after which a new session ID is sent to the FPolicy server during reconnection attempts. If the connection between the storage controller and the FPolicy server is terminated and reconnection is made within the -session-timeout interval, the old session ID is sent to FPolicy server so that it can send responses for old notifications. The default value is set to 10 seconds.</td>
<td></td>
</tr>
</tbody>
</table>
Related concepts

Additional information about configuring FPolicy external engines to use SSL authenticated connections on page 469
Restrictions for cluster-scoped FPolicy external engines with MetroCluster and SVM disaster recovery configurations on page 470

Related information

Clustered Data ONTAP 8.3 System Administration Guide

Additional information about configuring FPolicy external engines to use SSL authenticated connections

You need to know some additional information if you want to configure the FPolicy external engine to use SSL when connecting to FPolicy servers.

SSL server authentication

If you choose to configure the FPolicy external engine for SSL server authentication, before creating the external engine, you must install the public certificate of the certificate authority (CA) that signed the FPolicy server certificate.

Mutual authentication

If you configure FPolicy external engines to use SSL mutual authentication when connecting Storage Virtual Machine (SVM) data LIFs to external FPolicy servers, before creating the external engine, you must install the public certificate of the CA that signed the FPolicy server certificate along with the public certificate and key file for authentication of the SVM. You must not delete this certificate while any FPolicy policies are using the installed certificate.

If the certificate is deleted while FPolicy is using it for mutual authentication when connecting to an external FPolicy server, you cannot reenable a disabled FPolicy policy that uses that certificate. The FPolicy policy cannot be reenabled in this situation even if a new certificate with the same settings is created and installed on the SVM.

If the certificate has been deleted, you need to install a new certificate, create new FPolicy external engines that use the new certificate, and associate the new external engines with the FPolicy policy that you want to reenable by modifying the FPolicy policy.

How to install certificates for SSL

The public certificate of the CA that is used to sign the FPolicy server certificate is installed by using the `security certificate install` command with the `-type` parameter set to `client_ca`. The private key and public certificate required for authentication of the SVM is installed by using the `security certificate install` command with the `-type` parameter set to `server`.

Related concepts

Planning the FPolicy external engine configuration on page 464

Certificates do not replicate in SVM disaster recovery relationships with a non-ID-preserve configuration

Security certificates used for SSL authentication when making connections to FPolicy servers do not replicate to SVM disaster recovery destinations with non-ID-preserve configurations. Although the
FPolicy external-engine configuration on the SVM is replicated, security certificates are not replicated. You must manually install the security certificates on the destination.

When you set up the SVM disaster recovery relationship, the value you select for the -identity-preserve option of the snapmirror create command determines the configuration details that are replicated in the destination SVM.

If you set the -identity-preserve option to true (ID-preserve), all of the FPolicy configuration details are replicated, including the security certificate information. You must install the security certificates on the destination only if you set the option to false (non-ID-preserve).

Restrictions for cluster-scoped FPolicy external engines with MetroCluster and SVM disaster recovery configurations

You can create a cluster-scoped FPolicy external engine by assigning the cluster Storage Virtual Machine (SVM) to the external engine. However, when creating a cluster-scoped external engine in a MetroCluster or SVM disaster recovery configuration, there are certain restrictions when choosing the authentication method that the SVM uses for external communication with the FPolicy server.

There are three authentication options that you can choose when creating external FPolicy servers: no authentication, SSL server authentication, and SSL mutual authentication. Although there are no restrictions when choosing the authentication option if the external FPolicy server is assigned to a data SVM, there are restrictions when creating a cluster-scoped FPolicy external engine:

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Permitted?</th>
</tr>
</thead>
<tbody>
<tr>
<td>MetroCluster or SVM disaster recovery and a cluster-scoped FPolicy external engine with no authentication (SSL is not configured)</td>
<td>Yes</td>
</tr>
<tr>
<td>MetroCluster or SVM disaster recovery and a cluster-scoped FPolicy external engine with SSL server or SSL mutual authentication</td>
<td>No</td>
</tr>
</tbody>
</table>

- If a cluster-scoped FPolicy external engine with SSL authentication exists and you want to create a MetroCluster or SVM disaster recovery configuration, you must modify this external engine to use no authentication or remove the external engine before you can create the MetroCluster or SVM disaster recovery configuration.
- If the MetroCluster or SVM disaster recovery configuration already exists, clustered Data ONTAP prevents you from creating a cluster-scoped FPolicy external engine with SSL authentication.

Related concepts

Planning the FPolicy external engine configuration on page 464

Completing the FPolicy external engine configuration worksheet

You can use this worksheet to record the values that you need during the FPolicy external engine configuration process. If a parameter value is required, you need to determine what value to use for those parameters before you configure the external engine.

Information for a basic external engine configuration

You should record whether you want to include each parameter setting in the external engine configuration and then record the value for the parameters that you want to include.
<table>
<thead>
<tr>
<th>Type of information</th>
<th>Required</th>
<th>Include</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Virtual Machine (SVM) name</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Engine name</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Primary FPolicy servers</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Port number</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Secondary FPolicy servers</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>External engine type</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSL option for communication with external FPolicy server</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Certificate FQDN or custom common name</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificate serial number</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificate authority</td>
<td>No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Information for advanced external engine parameters**

To configure an external engine with advanced parameters, you must enter the configuration command while in advanced privilege mode.

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Required</th>
<th>Include</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout for canceling a request</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timeout for aborting a request</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interval for sending status requests</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum outstanding requests on the FPolicy server</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timeout for disconnecting a nonresponsive FPolicy server</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interval for sending keep-alive messages to the FPolicy server</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum reconnect attempts</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Receive buffer size</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send buffer size</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timeout for purging a session ID during reconnection</td>
<td>No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Planning the FPolicy event configuration

Before you configure FPolicy events, you must understand what it means to create an FPolicy event. You must determine which protocols you want the event to monitor, which events to monitor, and which event filters to use. This information helps you plan the values that you want to set.

What it means to create an FPolicy event

Creating the FPolicy event means defining information that the FPolicy process needs to determine what file access operations to monitor and for which of the monitored events notifications should be sent to the external FPolicy server. The FPolicy event configuration defines the following configuration information:

- Storage Virtual Machine (SVM) name
- Event name
- Which protocols to monitor
  FPolicy can monitor SMB, NFSv3, and NFSv4 file access operations.
- Which file operations to monitor
  Not all file operations are valid for each protocol.
- Which file filters to configure
  Only certain combinations of file operations and filters are valid. Each protocol has its own set of supported combinations.
- Whether to monitor volume mount and unmount operations

Note: There is a dependency with three of the parameters (-protocol, -file-operations, -filters). The following are the valid combinations for the three parameters:

- You can specify the -protocol and -file-operations parameters.
- You can specify all three of the parameters.
- You can specify none of the parameters.

What the FPolicy event configuration contains

You can use the following list of available FPolicy event configuration parameters to help you plan your configuration:

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVM</td>
<td>-vserver vserver_name</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specifies the SVM name</td>
</tr>
<tr>
<td></td>
<td>that you want to</td>
</tr>
<tr>
<td></td>
<td>associate with this</td>
</tr>
<tr>
<td></td>
<td>FPolicy event.</td>
</tr>
<tr>
<td></td>
<td>Each FPolicy configuration is defined within a single SVM. The external engine, policy event, policy scope, and policy that combine together to create an FPolicy policy configuration must all be associated with the same SVM.</td>
</tr>
<tr>
<td>Type of information</td>
<td>Option</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td><strong>Event name</strong></td>
<td>-event-name</td>
</tr>
<tr>
<td>Specifies the name to assign to the FPolicy event. When you create the FPolicy policy you associate the FPolicy event with the policy using the event name. The name can be up to 256 characters long. <strong>Note:</strong> The name should be up to 200 characters long if configuring the event in a MetroCluster or SVM disaster recovery configuration. The name can contain any combination of the following ASCII-range characters:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>event_name</td>
</tr>
<tr>
<td></td>
<td>• a through z</td>
</tr>
<tr>
<td></td>
<td>• A through Z</td>
</tr>
<tr>
<td></td>
<td>• 0 through 9</td>
</tr>
<tr>
<td></td>
<td>• &quot; _ - .“”</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>-protocol</td>
</tr>
<tr>
<td>Specifies which protocol to configure for the FPolicy event. The list for -protocol can include one of the following values:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>protocol</td>
</tr>
<tr>
<td></td>
<td>• cifs</td>
</tr>
<tr>
<td></td>
<td>• nfsv3</td>
</tr>
<tr>
<td></td>
<td>• nfsv4</td>
</tr>
</tbody>
</table>
| **Note:** If you specify -protocol, then you must specify a valid value in the -file-operations parameter. As the protocol version changes, the valid values might change.
<table>
<thead>
<tr>
<th>Type of information</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File operations</strong></td>
<td>-file-operations file_operations...</td>
</tr>
</tbody>
</table>

Specifies the list of file operations for the FPolicy event. The event checks the operations specified in this list from all client requests using the protocol specified in the `-protocol` parameter. You can list one or more file operations by using a comma-delimited list. The list for `-file-operations` can include one or more of the following values:

- `close` for file close operations
- `create` for file create operations
- `create-dir` for directory create operations
- `delete` for file delete operations
- `delete_dir` for directory delete operations
- `getattr` for get attribute operations
- `link` for link operations
- `lookup` for lookup operations
- `open` for file open operations
- `read` for file read operations
- `write` for file write operations
- `rename` for file rename operations
- `rename_dir` for directory rename operations
- `setattr` for set attribute operations
- `symlink` for symbolic link operations

**Note:** If you specify `-file-operations`, then you must specify a valid protocol in the `-protocol` parameter.
### Type of information

**Filters**
Specifies the list of filters for a given file operation for the specified protocol. The values in the `-filters` parameter are used to filter client requests. The list can include one or more of the following:

- **monitor-ads** to filter the client request for alternate data stream
- **close-with-modification** to filter the client request for close with modification
- **close-without-modification** to filter the client request for close without modification
- **first-read** to filter the client request for first read
- **first-write** to filter the client request for first write
- **offline-bit** to filter the client request for offline bit set
  Setting this filter results in the FPolicy server receiving notification only when offline files are accessed.
- **open-with-delete-intent** to filter the client request for open with delete intent
  Setting this filter results in the FPolicy server receiving notification only when an attempt is made to open a file with the intent to delete it. This is used by file systems when the `FILE_DELETE_ON_CLOSE` flag is specified.
- **open-with-write-intent** to filter client request for open with write intent
  Setting this filter results in the FPolicy server receiving notification only when an attempt is made to open a file with the intent to write something in it.
- **write-with-size-change** to filter the client request for write with size change

**Note:** If you specify the `-filters` parameter, then you must also specify valid values for the `-file-operations` and `-protocol` parameters.

<table>
<thead>
<tr>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-filters filter,...</code></td>
</tr>
</tbody>
</table>

### Is volume operation required
Specifies whether monitoring is required for volume mount and unmount operations. The default is `false`.

<table>
<thead>
<tr>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>`-volume-operation {true</td>
</tr>
</tbody>
</table>

---

### List of supported file operation and filter combinations that FPolicy can monitor for SMB

When you configure your FPolicy event, you need to be aware that only certain combinations of file operations and filters are supported for monitoring SMB file access operations.

The list of supported file operation and filter combinations for FPolicy monitoring of SMB file access events is provided in the following table:

<table>
<thead>
<tr>
<th>Supported file operations</th>
<th>Supported filters</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>close</code></td>
<td><code>monitor-ads, offline-bit, close-with-modification, close-without-modification</code></td>
</tr>
</tbody>
</table>
List of supported file operation and filter combinations that FPolicy can monitor for NFSv3

When you configure your FPolicy event, you need to be aware that only certain combinations of file operations and filters are supported for monitoring NFSv3 file access operations.

The list of supported file operation and filter combinations for FPolicy monitoring of NFSv3 file access events is provided in the following table:

<table>
<thead>
<tr>
<th>Supported file operations</th>
<th>Supported filters</th>
</tr>
</thead>
<tbody>
<tr>
<td>create</td>
<td>monitor-ads, offline-bit</td>
</tr>
<tr>
<td>create_dir</td>
<td>Currently no filter is supported for this file operation.</td>
</tr>
<tr>
<td>delete</td>
<td>monitor-ads, offline-bit</td>
</tr>
<tr>
<td>delete_dir</td>
<td>Currently no filter is supported for this file operation.</td>
</tr>
<tr>
<td>getattr</td>
<td>offline-bit</td>
</tr>
<tr>
<td>open</td>
<td>monitor-ads, offline-bit, open-with-delete-intent, open-with-write-intent</td>
</tr>
<tr>
<td>read</td>
<td>monitor-ads, offline-bit, first-read</td>
</tr>
<tr>
<td>write</td>
<td>monitor-ads, offline-bit, first-write, write-with-size-change</td>
</tr>
<tr>
<td>rename</td>
<td>monitor-ads, offline-bit</td>
</tr>
<tr>
<td>rename_dir</td>
<td>Currently no filter is supported for this file operation.</td>
</tr>
<tr>
<td>setattr</td>
<td>offline-bit</td>
</tr>
<tr>
<td>symlink</td>
<td>offline-bit</td>
</tr>
</tbody>
</table>

List of supported file operation and filter combinations that FPolicy can monitor for NFSv4

When you configure your FPolicy event, you need to be aware that only certain combinations of file operations and filters are supported for monitoring NFSv4 file access operations.

The list of supported file operation and filter combinations for FPolicy monitoring of NFSv4 file access events is provided in the following table:

<table>
<thead>
<tr>
<th>Supported file operations</th>
<th>Supported filters</th>
</tr>
</thead>
<tbody>
<tr>
<td>create</td>
<td>offline-bit</td>
</tr>
<tr>
<td>create_dir</td>
<td>Currently no filter is supported for this file operation.</td>
</tr>
<tr>
<td>delete</td>
<td>offline-bit</td>
</tr>
<tr>
<td>delete_dir</td>
<td>Currently no filter is supported for this file operation.</td>
</tr>
<tr>
<td>link</td>
<td>offline-bit</td>
</tr>
<tr>
<td>lookup</td>
<td>offline-bit</td>
</tr>
<tr>
<td>read</td>
<td>offline-bit</td>
</tr>
<tr>
<td>write</td>
<td>offline-bit, write-with-size-change</td>
</tr>
<tr>
<td>rename</td>
<td>offline-bit</td>
</tr>
<tr>
<td>rename_dir</td>
<td>Currently no filter is supported for this file operation.</td>
</tr>
<tr>
<td>setattr</td>
<td>offline-bit</td>
</tr>
<tr>
<td>symlink</td>
<td>offline-bit</td>
</tr>
</tbody>
</table>
**Supported file operations** | **Supported filters**  
--- | ---  
close | offline-bit  
create | offline-bit  
create_dir | Currently no filter is supported for this file operation.  
delete | offline-bit  
delete_dir | Currently no filter is supported for this file operation.  
getattr | offline-bit  
link | offline-bit  
lookup | offline-bit  
open | offline-bit  
read | offline-bit  
write | offline-bit, write-with-size-change  
rename | offline-bit  
rename_dir | Currently no filter is supported for this file operation.  
setattr | offline-bit  
symlink | offline-bit  
  
**Completing the FPolicy event configuration worksheet**

You can use this worksheet to record the values that you need during the FPolicy event configuration process. If a parameter value is required, you need to determine what value to use for those parameters before you configure the FPolicy event.

You should record whether you want to include each parameter setting in the FPolicy event configuration and then record the value for the parameters that you want to include.

<table>
<thead>
<tr>
<th><strong>Type of information</strong></th>
<th><strong>Required</strong></th>
<th><strong>Include</strong></th>
<th><strong>Your values</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Virtual Machine (SVM) name</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Event name</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File operations</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Filters</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is volume operation required</td>
<td>No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Planning the FPolicy policy configuration**

Before you configure the FPolicy policy, you must understand which parameters are required when creating the policy as well as why you might want to configure certain optional parameters. This information helps you to determine which values to set for each parameter.

When creating an FPolicy policy you associate the policy with the following:

- The Storage Virtual Machine (SVM)
- One or more FPolicy events
• An FPolicy external engine

You can also configure several optional policy settings.

**What the FPolicy policy configuration contains**

You can use the following list of available FPolicy policy required and optional parameters to help you plan your configuration:

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Option</th>
<th>Required</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVM name</td>
<td>-vserver vserver_name</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>Policy name</td>
<td>-policy-name policy_name</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>Event names</td>
<td>-events event_name,...</td>
<td>Yes</td>
<td>None</td>
</tr>
</tbody>
</table>

*SVM name*

Specifies the name of the SVM on which you want to create an FPolicy policy.

<table>
<thead>
<tr>
<th>Option</th>
<th>Required</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>-vserver vserver_name</td>
<td>Yes</td>
<td>None</td>
</tr>
</tbody>
</table>

*Policy name*

Specifies the name of the FPolicy policy. The name can be up to 256 characters long.

**Note:** The name should be up to 200 characters long if configuring the policy in a MetroCluster or SVM disaster recovery configuration.

The name can contain any combination of the following ASCII-range characters:

- a through z
- A through Z
- 0 through 9
- "", ",", and "."
<table>
<thead>
<tr>
<th>Type of information</th>
<th>Option</th>
<th>Required</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>External engine name</strong></td>
<td>-engine <code>engine_name</code></td>
<td>Yes (unless the policy uses the internal Data ONTAP native engine)</td>
<td>native</td>
</tr>
<tr>
<td>Specifies the name of the external engine to associate with the FPolicy policy.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• An external engine contains information required by the node to send notifications to an FPolicy server.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• You can configure FPolicy to use the Data ONTAP native external engine for simple file blocking or to use an external engine that is configured to use external FPolicy servers (FPolicy servers) for more sophisticated file blocking and file management.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• If you want to use the native external engine, you can either not specify a value for this parameter or you can specify native as the value.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• If you want to use FPolicy servers, the configuration for the external engine must already exist.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Is mandatory screening required</strong></td>
<td>-is-mandatory `true</td>
<td>false`</td>
<td>No</td>
</tr>
<tr>
<td>Specifies whether mandatory file access screening is required.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• The mandatory screening setting determines what action is taken on a file access event in a case when all primary and secondary servers are down or no response is received from the FPolicy servers within a given timeout period.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• When set to true, file access events are denied.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• When set to false, file access events are allowed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type of information</td>
<td>Option</td>
<td>Required</td>
<td>Default</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>----------------------------</td>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Allow privileged access</strong></td>
<td>-allow-privileged-access {yes</td>
<td>no}</td>
<td>No (unless passthrough-read is enabled)</td>
</tr>
<tr>
<td>Specifies whether you want the FPolicy server to have privileged access to the monitored files and folders by using a privileged data connection. If configured, FPolicy servers can access files from the root of the SVM containing the monitored data using the privileged data connection. For privileged data access, CIFS must be licensed on the cluster and all the data LIFs used to connect to the FPolicy servers must be configured to have cifs as one of the allowed protocols. If you want to configure the policy to allow privileged access, you must also specify the user name for the account that you want the FPolicy server to use for privileged access.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Privileged user name</strong></td>
<td>-privileged-user-name user_name</td>
<td>No (unless privileged access is enabled)</td>
<td>None</td>
</tr>
<tr>
<td>Specifies the user name of the account the FPolicy servers use for privileged data access. • The value for this parameter should use the &quot;domain\user name&quot; format. • If -allow-privileged-access is set to no, any value set for this parameter is ignored.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Type of information | Option | Required | Default
--- | --- | --- | ---
Allow passthrough-read | -is-passthrough-read-enabled {true|false} | No | false

**Related concepts**

- *How FPolicy manages policy processing* on page 456
- *Requirements, considerations, and best practices for configuring FPolicy* on page 461
- *How FPolicy passthrough-read enhances usability for hierarchical storage management* on page 459
- *Requirement for FPolicy scope configurations if the FPolicy policy uses the native engine* on page 481

**Requirement for FPolicy scope configurations if the FPolicy policy uses the native engine**

If you configure the FPolicy policy to use the native engine, there is a specific requirement for how you define the FPolicy scope configured for the policy.

The FPolicy scope defines the boundaries on which the FPolicy policy applies, for example whether the FPolicy applies to specified volumes or shares. There are a number of parameters that further restrict the scope to which the FPolicy policy applies. One of these parameters, -is-file-extension-check-on-directories-enabled, specifies whether to check file extensions on directories. The default value is **false**, which means that file extensions on directories are not checked.

When an FPolicy policy that uses the native engine is enabled on a share or volume and the -is-file-extension-check-on-directories-enabled parameter is set to **false** for the scope of the policy, directory access is denied. With this configuration, because the file extensions are not checked for directories, any directory operation is denied if it falls under the scope of the policy.

To ensure that directory access succeeds when using the native engine, you must set the -is-file-extension-check-on-directories-enabled parameter to **true** when creating the scope.
With this parameter set to true, extension checks happen for directory operations and the decision whether to allow or deny access is taken based on the extensions included or excluded in the FPolicy scope configuration.

Related concepts

- FPolicy configuration types on page 458
- When to create a native FPolicy configuration on page 459
- Planning the FPolicy scope configuration on page 482

Completing the FPolicy policy worksheet

You can use this worksheet to record the values that you need during the FPolicy policy configuration process. You should record whether you want to include each parameter setting in the FPolicy policy configuration and then record the value for the parameters that you want to include.

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Include</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Virtual Machine (SVM) name</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Policy name</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Event names</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>External engine name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is mandatory screening required</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow privileged access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privileged user name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is passthrough-read enabled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Planning the FPolicy scope configuration

Before you configure the FPolicy scope, you must understand what it means to create a scope. You must understand what the scope configuration contains. You also need to understand what the scope rules of precedence are. This information can help you plan the values that you want to set.

What it means to create an FPolicy scope

Creating the FPolicy scope means defining the boundaries on which the FPolicy policy applies. The Storage Virtual Machine (SVM) is the basic boundary. When you create a scope for an FPolicy policy, you must define the FPolicy policy to which it will apply, and you must designate to which SVM you want to apply the scope.

There are a number of parameters that further restrict the scope within the specified SVM. You can restrict the scope by specifying what to include in the scope or by specifying what to exclude from the scope. After you apply a scope to an enabled policy, policy event checks get applied to the scope defined by this command.

Notifications are generated for file access events where matches are found in the “include” options. Notifications are not generated for file access events where matches are found in the “exclude” options.

The FPolicy scope configuration defines the following configuration information:

- SVM name
- Policy name
- The shares to include or exclude from what gets monitored
- The export policies to include or exclude from what gets monitored
- The volumes to include or exclude from what gets monitored
- The file extensions to include or exclude from what gets monitored
- Whether to do file extension checks on directory objects

**Note:** There are special considerations for the scope for a cluster FPolicy policy. The cluster FPolicy policy is a policy that the cluster administrator creates for the admin SVM. If the cluster administrator also creates the scope for that cluster FPolicy policy, the SVM administrator cannot create a scope for that same policy. However, if the cluster administrator does not create a scope for the cluster FPolicy policy, then any SVM administrator can create the scope for that cluster policy. If the SVM administrator creates a scope for that cluster FPolicy policy, the cluster administrator cannot subsequently create a cluster scope for that same cluster policy. This is because the cluster administrator cannot override the scope for the same cluster policy.

**What the scope rules of precedence are**

The following rules of precedence apply to scope configurations:

- When a share is included in the `-shares-to-include` parameter and the parent volume of the share is included in the `-volumes-to-exclude` parameter, `-volumes-to-exclude` has precedence over `-shares-to-include`.
- When an export policy is included in the `-export-policies-to-include` parameter and the parent volume of the export policy is included in the `-volumes-to-exclude` parameter, `-volumes-to-exclude` has precedence over `-export-policies-to-include`.
- An administrator can specify both `-file-extensions-to-include` and `-file-extensions-to-exclude` lists. The `-file-extensions-to-exclude` parameter is checked before the `-file-extensions-to-include` parameter is checked.

**What the FPolicy scope configuration contains**

You can use the following list of available FPolicy scope configuration parameters to help you plan your configuration:

**Note:** When configuring what shares, export policies, volumes, and file extensions to include or exclude from the scope, the include and exclude parameters can contain regular expressions and can include metacharacters such as “?” and “*”.

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SVM</strong></td>
<td>-vserver vserver_name</td>
</tr>
<tr>
<td>Specifies the SVM name on which you want to create an FPolicy scope. Each FPolicy configuration is defined within a single SVM. The external engine, policy event, policy scope, and policy that combine together to create an FPolicy policy configuration must all be associated with the same SVM.</td>
<td></td>
</tr>
<tr>
<td><strong>Policy name</strong></td>
<td>-policy-name policy_name</td>
</tr>
<tr>
<td>Specifies the name of the FPolicy policy to which you want to attach the scope. The FPolicy policy must already exist.</td>
<td></td>
</tr>
<tr>
<td><strong>Shares to include</strong></td>
<td>-shares-to-include share_name,...</td>
</tr>
<tr>
<td>Specifies a comma-delimited list of shares to monitor for the FPolicy policy to which the scope is applied.</td>
<td></td>
</tr>
<tr>
<td>Type of information</td>
<td>Option</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Shares to exclude</strong></td>
<td>-shares-to-exclude share_name,...</td>
</tr>
<tr>
<td>Specifies a comma-delimited list of</td>
<td></td>
</tr>
<tr>
<td>shares to exclude from monitoring</td>
<td></td>
</tr>
<tr>
<td>for the FPolicy policy to which</td>
<td></td>
</tr>
<tr>
<td>the scope is applied.</td>
<td></td>
</tr>
<tr>
<td><strong>Volumes to include</strong></td>
<td>-volumes-to-include volume_name,...</td>
</tr>
<tr>
<td>Specifies a comma-delimited list of</td>
<td></td>
</tr>
<tr>
<td>volumes to monitor for the FPolicy</td>
<td></td>
</tr>
<tr>
<td>policy to which the scope is applied.</td>
<td></td>
</tr>
<tr>
<td><strong>Volumes to exclude</strong></td>
<td>-volumes-to-exclude volume_name,...</td>
</tr>
<tr>
<td>Specifies a comma-delimited list of</td>
<td></td>
</tr>
<tr>
<td>volumes to exclude from monitoring</td>
<td></td>
</tr>
<tr>
<td>for the FPolicy policy to which</td>
<td></td>
</tr>
<tr>
<td>the scope is applied.</td>
<td></td>
</tr>
<tr>
<td><strong>Export policies to include</strong></td>
<td>-export-policies-to-include export_policy_name,...</td>
</tr>
<tr>
<td>Specifies a comma-delimited list of</td>
<td></td>
</tr>
<tr>
<td>export policies to monitor for the</td>
<td></td>
</tr>
<tr>
<td>FPolicy policy to which the scope</td>
<td></td>
</tr>
<tr>
<td>is applied.</td>
<td></td>
</tr>
<tr>
<td><strong>Export policies to exclude</strong></td>
<td>-export-policies-to-exclude export_policy_name,...</td>
</tr>
<tr>
<td>Specifies a comma-delimited list of</td>
<td></td>
</tr>
<tr>
<td>export policies to exclude from</td>
<td></td>
</tr>
<tr>
<td>monitoring for the FPolicy policy</td>
<td></td>
</tr>
<tr>
<td>to which the scope is applied.</td>
<td></td>
</tr>
<tr>
<td><strong>File extensions to include</strong></td>
<td>-file-extensions-to-include file_extensions,...</td>
</tr>
<tr>
<td>Specifies a comma-delimited list of</td>
<td></td>
</tr>
<tr>
<td>file extensions to monitor for the</td>
<td></td>
</tr>
<tr>
<td>FPolicy policy to which the scope</td>
<td></td>
</tr>
<tr>
<td>is applied.</td>
<td></td>
</tr>
<tr>
<td><strong>File extension to exclude</strong></td>
<td>-file-extensions-to-exclude file_extensions,...</td>
</tr>
<tr>
<td>Specifies a comma-delimited list of</td>
<td></td>
</tr>
<tr>
<td>file extensions to exclude from</td>
<td></td>
</tr>
<tr>
<td>monitoring for the FPolicy policy</td>
<td></td>
</tr>
<tr>
<td>to which the scope is applied.</td>
<td></td>
</tr>
<tr>
<td>**Is file extension check on</td>
<td>-is-file-extension-check-on-directories-enabled {true</td>
</tr>
<tr>
<td>directory enabled**</td>
<td></td>
</tr>
<tr>
<td>Specifies whether the file name</td>
<td></td>
</tr>
<tr>
<td>extension checks apply to directory</td>
<td></td>
</tr>
<tr>
<td>objects as well. If this parameter</td>
<td></td>
</tr>
<tr>
<td>is set to true, the directory</td>
<td></td>
</tr>
<tr>
<td>objects are subjected to the same</td>
<td></td>
</tr>
<tr>
<td>extension checks as regular files.</td>
<td></td>
</tr>
<tr>
<td>If this parameter is set to false,</td>
<td></td>
</tr>
<tr>
<td>the directory names are not matched</td>
<td></td>
</tr>
<tr>
<td>for extensions and notifications are</td>
<td></td>
</tr>
<tr>
<td>sent for directories even if their</td>
<td></td>
</tr>
<tr>
<td>name extensions do not match.</td>
<td></td>
</tr>
<tr>
<td>If the FPolicy policy to which the</td>
<td></td>
</tr>
<tr>
<td>scope is assigned is configured to</td>
<td></td>
</tr>
<tr>
<td>use the native engine, this parameter</td>
<td></td>
</tr>
<tr>
<td>must be set to true.</td>
<td></td>
</tr>
</tbody>
</table>

**Related concepts**

*Requirement for FPolicy scope configurations if the FPolicy policy uses the native engine* on page 481

**Completing the FPolicy scope worksheet**

You can use this worksheet to record the values that you need during the FPolicy scope configuration process. If a parameter value is required, you need to determine what value to use for those parameters before you configure the FPolicy scope.

You should record whether you want to include each parameter setting in the FPolicy scope configuration and then record the value for the parameters that you want to include.
### Creating the FPolicy configuration

There are several steps you must perform to creating an FPolicy configuration. First, you must plan your configuration. Then, you create an FPolicy external engine, an FPolicy event, and an FPolicy policy. You then create an FPolicy scope and attach it to the FPolicy policy, and then enable the FPolicy policy.

FPolicy is supported on Storage Virtual Machines (SVMs) with FlexVol volumes. FPolicy is not supported on SVMs with Infinite Volume.

**Steps**

1. **Creating the FPolicy external engine** on page 486
   
   The first step to creating an FPolicy configuration is to create an external engine. The external engine defines how FPolicy makes and manages connections to external FPolicy servers. If your configuration uses the internal Data ONTAP engine (the native external engine) for simple file blocking, you do not need to configure a separate FPolicy external engine and do not need to perform this step.

2. **Creating the FPolicy event** on page 487
   
   As part of creating an FPolicy policy configuration, you need to create an FPolicy event. You associate the event with the FPolicy policy when it is created. An event defines which protocol to monitor and which file access events to monitor and filter.

3. **Creating the FPolicy policy** on page 487
   
   When you create the FPolicy policy, you associate an external engine and one or more events to the policy. The policy also specifies whether mandatory screening is required, whether the FPolicy servers have privileged access to data on the Storage Virtual Machine (SVM), and whether passthrough-read for offline files is enabled.

4. **Creating the FPolicy scope** on page 489
   
   After creating the FPolicy policy, you need to create an FPolicy scope. When creating the scope, you associate the scope with an FPolicy policy. A scope defines the boundaries on which the FPolicy policy applies. Scopes can include or exclude files based on shares, export policies, volumes, and file extensions.

5. **Enabling the FPolicy policy** on page 489

---

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Required</th>
<th>Include</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Virtual Machine (SVM) name</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Policy name</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Shares to include</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shares to exclude</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Volumes to include</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Volumes to exclude</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Export policies to include</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Export policies to exclude</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File extensions to include</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File extension to exclude</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is file extension check on directory enabled</td>
<td>No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
After you are through configuring an FPolicy policy configuration, you enable the FPolicy policy. Enabling the policy sets its priority and starts file access monitoring for the policy.

Related concepts
- What the steps for setting up an FPolicy configuration are on page 463
- Planning the FPolicy configuration on page 464
- Requirements, considerations, and best practices for configuring FPolicy on page 461
- Displaying information about FPolicy configurations on page 491
- How FPolicy passthrough-read enhances usability for hierarchical storage management on page 459

Creating the FPolicy external engine

The first step to creating an FPolicy configuration is to create an external engine. The external engine defines how FPolicy makes and manages connections to external FPolicy servers. If your configuration uses the internal Data ONTAP engine (the native external engine) for simple file blocking, you do not need to configure a separate FPolicy external engine and do not need to perform this step.

Before you begin

The external engine worksheet should be completed.

About this task

If the external engine is used in a MetroCluster configuration, you should specify the IP addresses of the FPolicy servers at the source site as primary servers. The IP addresses of the FPolicy servers at the destination site should be specified as secondary servers.

Steps

1. Create the FPolicy external engine by using the `vserver fpolicy policy external-engine create` command.

   Example

   The following command creates an external engine on Storage Virtual Machine (SVM) vs1.example.com. No authentication is required for external communications with the FPolicy server.

   ```bash
   vserver fpolicy policy external-engine create -vserver-name vs1.example.com -engine-name engine1 -primary-servers 10.1.1.2,10.1.1.3 -port 6789 -ssl-option no-auth
   ```

2. Verify the FPolicy external engine configuration by using the `vserver fpolicy policy external-engine show` command.

   Example

   The following command display information about all external engines configured on SVM vs1.example.com:

   ```bash
   vserver fpolicy policy external-engine show -vserver vs1.example.com
   ```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Engine</th>
<th>Primary Servers</th>
<th>Secondary Servers</th>
<th>Port</th>
<th>Engine Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1.example.com</td>
<td>engine1</td>
<td>10.1.1.2,</td>
<td>-</td>
<td>6789</td>
<td>synchronous</td>
</tr>
</tbody>
</table>
The following command displays detailed information about the external engine named “engine1” on SVM vs1.example.com:

```
vserver fpolicy policy external-engine show -vserver vs1.example.com -engine-name engine1
```

```
Vserver: vs1.example.com
Engine: engine1
Primary FPolicy Servers: 10.1.1.2, 10.1.1.3
Port Number of FPolicy Service: 6789
Secondary FPolicy Servers: -
External Engine Type: synchronous
SSL Option for External Communication: no-auth
FQDN or Custom Common Name: -
Serial Number of Certificate: -
Certificate Authority: -
```

Creating the FPolicy event

As part of creating an FPolicy policy configuration, you need to create an FPolicy event. You associate the event with the FPolicy policy when it is created. An event defines which protocol to monitor and which file access events to monitor and filter.

**Before you begin**

The FPolicy event worksheet should be completed.

**Steps**

1. Create the FPolicy event by using the `vserver fpolicy policy event create` command.

   **Example**
   
   ```
vserver fpolicy policy event create -vserver-name vs1.example.com -event-name event1 -protocol cifs -file-operations open,close,read,write
   ```

2. Verify the FPolicy event configuration by using the `vserver fpolicy policy event show` command.

   **Example**
   
   ```
vserver fpolicy policy event show -vserver vs1.example.com
   ```

```
<table>
<thead>
<tr>
<th>Vserver</th>
<th>Event Name</th>
<th>Protocols</th>
<th>File Operations</th>
<th>Filters</th>
<th>Is Volume Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1.example.com</td>
<td>event1</td>
<td>cifs</td>
<td>open, close, read, write</td>
<td>-</td>
<td>false</td>
</tr>
</tbody>
</table>
```

Creating the FPolicy policy

When you create the FPolicy policy, you associate an external engine and one or more events to the policy. The policy also specifies whether mandatory screening is required, whether the FPolicy servers have privileged access to data on the Storage Virtual Machine (SVM), and whether passthrough-read for offline files is enabled.

**Before you begin**

- The FPolicy policy worksheet should be completed.
- If you plan on configuring the policy to use FPolicy servers, the external engine must exist.
• At least one FPolicy event that you plan on associating with the FPolicy policy must exist.

• If you want to configure privileged data access, a CIFS server must exist on the SVM.

Steps

1. Create the FPolicy policy:

   ```
   vserver fpolicy policy create -vserver-name vserver_name -policy-name policy_name -engine engine_name -events event_name,... [-is-mandatory {true|false}] [-allow-privileged-access {yes|no}] [-privileged-user-name domain\user_name] [-is-passthrough-read-enabled {true|false}]
   ```

   • You can add one or more events to the FPolicy policy.
   
   • By default, mandatory screening is enabled.
   
   • If you want to allow privileged access by setting the -allow-privileged-access parameter to yes, you must also configure a privileged user name for privileged access.
   
   • If you want to configure passthrough-read by setting the -is-passthrough-read-enabled parameter to true, you must also configure privileged data access.

Example

The following command creates a policy named “policy1” that has the event named “event1” and the external engine named “engine1” associated with it. This policy uses default values in the policy configuration:

   ```
   vserver fpolicy policy create -vserver vs1.example.com -policy-name policy1 -events event1 -engine engine1
   ```

   The following command creates a policy named “policy2” that has the event named “event2” and the external engine named “engine2” associated with it. This policy is configured to use privileged access using the specified user name. Passthrough-read is enabled:

   ```
   vserver fpolicy policy create -vserver vs1.example.com -policy-name policy2 -events event2 -engine engine2 -allow-privileged-access yes -privileged-user-name example\archive_acct -is-passthrough-read-enabled true
   ```

   The following command creates a policy named “native1” that has the event named “event3” associated with it. This policy uses the native engine and uses default values in the policy configuration:

   ```
   vserver fpolicy policy create -vserver vs1.example.com -policy-name native1 -events event3 -engine native
   ```

2. Verify the FPolicy policy configuration by using the vserver fpolicy policy show command.

Example

The following command displays information about the three configured Fpolicy polices, including the following information:

• The SVM associated with the policy

• The external engine associated with the policy

• The events associated with the policy

• Whether mandatory screening is required

• Whether privileged access is required
Creating the FPolicy scope

After creating the FPolicy policy, you need to create an FPolicy scope. When creating the scope, you associate the scope with an FPolicy policy. A scope defines the boundaries on which the FPolicy policy applies. Scopes can include or exclude files based on shares, export policies, volumes, and file extensions.

Before you begin

The FPolicy scope worksheet must be completed. The FPolicy policy must exist with an associated external engine (if the policy is configured to use external FPolicy servers) and must have at least one associated FPolicy event.

Steps

1. Create the FPolicy scope by using the `vserver fpolicy policy scope create` command.

   Example
   
   ```bash
   vserver fpolicy policy scope create -vserver-name vs1.example.com -policy-name policy1 -volumes-to-include datavol1, datavol2
   ```

2. Verify the FPolicy scope configuration by using the `vserver fpolicy policy scope show` command.

   Example
   
   ```bash
   vserver fpolicy policy scope show -vserver vs1.example.com -instance
   ```

Enabling the FPolicy policy

After you are through configuring an FPolicy policy configuration, you enable the FPolicy policy. Enabling the policy sets its priority and starts file access monitoring for the policy.

Before you begin

The FPolicy policy must exist with an associated external engine (if the policy is configured to use external FPolicy servers) and must have at least one associated FPolicy event. The FPolicy policy scope must exist and must be assigned to the FPolicy policy.
About this task

The priority is used when multiple policies are enabled on the Storage Virtual Machine (SVM) and more than one policy has subscribed to the same file access event. Policies that use the native engine configuration have a higher priority than policies for any other engine, regardless of the sequence number assigned to them when enabling the policy.

Note: A policy cannot be enabled on the admin SVM.

Steps

1. Enable the FPolicy policy by using the `vserver fpolicy enable` command.

   Example
   
   ```
   vserver fpolicy enable -vserver-name vs1.example.com -policy-name policy1 -sequence-number 1
   ```

2. Verify that the FPolicy policy is enabled by using the `vserver fpolicy show` command.

   Example
   
   ```
   vserver fpolicy show -vserver vs1.example.com
   ```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Policy Name</th>
<th>Sequence Number</th>
<th>Status</th>
<th>Engine</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1.example.com</td>
<td>policy1</td>
<td>1</td>
<td>on</td>
<td>engine1</td>
</tr>
</tbody>
</table>

Modifying FPolicy configurations

You can modify FPolicy configurations by modifying the elements that make up the configuration. You can modify external engines, FPolicy events, FPolicy scopes, and FPolicy policies. You can also enable or disable FPolicy policies. When you disable the FPolicy policy, file monitoring is discontinued for that policy.

It is recommended to disable the FPolicy policy before modifying the configuration.

Related concepts

- Creating the FPolicy configuration on page 485
- Managing FPolicy server connections on page 494

Commands for modifying FPolicy configurations

You can modify FPolicy external engines, events, scopes, and policies.

<table>
<thead>
<tr>
<th>If you want to modify...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>External engines</td>
<td>vserver fpolicy policy external-engine modify</td>
</tr>
<tr>
<td>Events</td>
<td>vserver fpolicy policy event modify</td>
</tr>
<tr>
<td>Scopes</td>
<td>vserver fpolicy policy scope modify</td>
</tr>
<tr>
<td>Policies</td>
<td>vserver fpolicy policy modify</td>
</tr>
</tbody>
</table>

See the man pages for the commands for more information.
Enabling or disabling FPolicy policies

You can enable FPolicy policies after the configuration is complete. Enabling the policy sets its priority and starts file access monitoring for the policy. You can disable FPolicy policies if you want to stop file access monitoring for the policy.

Before you begin

Before enabling FPolicy policies, the FPolicy configuration must be completed.

About this task

- The priority is used when multiple policies are enabled on the Storage Virtual Machine (SVM) and more than one policy has subscribed to the same file access event.
- Policies that use the native engine configuration have a higher priority than policies for any other engine, regardless of the sequence number assigned to them when enabling the policy.
- If you want to change the priority of an FPolicy policy, you must disable the policy and then reenable it using the new sequence number.

Step

1. Perform the appropriate action:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Enter the following command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable an FPolicy policy</td>
<td><code>vserver fpolicy enable -vserver-name vserver_name -policy-name policy_name -sequence-number integer</code></td>
</tr>
<tr>
<td>Disable an FPolicy policy</td>
<td><code>vserver fpolicy disable -vserver-name vserver_name -policy-name policy_name</code></td>
</tr>
</tbody>
</table>

Related tasks

- Displaying information about FPolicy policy status on page 492
- Displaying information about enabled FPolicy policies on page 493

Displaying information about FPolicy configurations

You might want to display information about FPolicy configurations to determine whether the configuration for each Storage Virtual Machine (SVM) is correct or to verify that an FPolicy policy configuration is enabled. You can display information about FPolicy external engines, FPolicy events, FPolicy scopes, and FPolicy policies.

Related concepts

- Creating the FPolicy configuration on page 485
- Modifying FPolicy configurations on page 490
How the show commands work

It is helpful when displaying information about the FPolicy configuration to understand how the show commands work.

A show command without additional parameters displays information in a summary form. Additionally, every show command has the same two mutually exclusive optional parameters, -instance and -fields.

When you use the -instance parameter with a show command, the command output displays detailed information in a list format. In some cases, the detailed output can be lengthy and include more information than you need. You can use the -fields fieldname[,fieldname...] parameter to customize the output so that it displays information only for the fields you specify. You can identify which fields that you can specify by entering ? after the -fields parameter.

Note: The output of a show command with the -fields parameter might display other relevant and necessary fields related to the requested fields.

Every show command has one or more optional parameters that filter that output and enable you to narrow the scope of information displayed in command output. You can identity which optional parameters are available for a command by entering ? after the show command.

The show command supports UNIX-style patterns and wildcards to enable you to match multiple values in command-parameters arguments. For example, you can use the wildcard operator (*), the NOT operator (!), the OR operator (|), the range operator (integer...integer), the less-than operator (<), the greater-than operator (>), the less-than or equal to operator (<=), and the greater-than or equal to operator (>=) when specifying values.

For more information about using UNIX-style patterns and wildcards, see the “Using the Data ONTAP command-line interface” section of the Clustered Data ONTAP System Administration Guide for SVM Administrators.

Commands for displaying information about FPolicy configurations

You use the fpolicy show commands to display information about the FPolicy configuration, including information about FPolicy external engines, events, scopes, and policies.

<table>
<thead>
<tr>
<th>If you want to display information about FPolicy...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>External engines</td>
<td>vserver fpolicy policy external-engine show</td>
</tr>
<tr>
<td>Events</td>
<td>vserver fpolicy policy event show</td>
</tr>
<tr>
<td>Scopes</td>
<td>vserver fpolicy policy scope show</td>
</tr>
<tr>
<td>Policies</td>
<td>vserver fpolicy policy show</td>
</tr>
</tbody>
</table>

See the man pages for the commands for more information.

Displaying information about FPolicy policy status

You can display information about the status for FPolicy policies to determine whether a policy is enabled, what external engine it is configured to use, what the sequence number is for the policy, and to which Storage Virtual Machine (SVM) the FPolicy policy is associated.

About this task

If you do not specify any parameters, the command displays the following information:

- SVM name
• Policy name
• Policy sequence number
• Policy status

In addition to displaying information about policy status for FPolicy policies configured on the cluster or a specific SVM, you can use command parameters to filter the command’s output by other criteria.

You can specify the `-instance` parameter to display detailed information about listed policies. Alternatively, you can use the `-fields` parameter to display only the indicated fields in the command output, or `-fields ?` to determine what fields you can use.

**Step**

1. Display filtered information about FPolicy policy status by using the appropriate command:

<table>
<thead>
<tr>
<th>If you want to display status information about policies...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>On the cluster</td>
<td><code>vserver fpolicy show</code></td>
</tr>
<tr>
<td>That have the specified status</td>
<td>`vserver fpolicy show -status {on</td>
</tr>
<tr>
<td>On a specified SVM</td>
<td><code>vserver fpolicy show -vserver vserver_name</code></td>
</tr>
<tr>
<td>With the specified policy name</td>
<td><code>vserver fpolicy show -policy-name policy_name</code></td>
</tr>
<tr>
<td>That use the specified external engine</td>
<td><code>vserver fpolicy show -engine engine_name</code></td>
</tr>
</tbody>
</table>

The following example displays the information about FPolicy policies on the cluster:

```
cluster1::> vserver fpolicy show

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Policy Name</th>
<th>Sequence Number</th>
<th>Status</th>
<th>Engine</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPolicy</td>
<td>cserver_policy</td>
<td>-</td>
<td>off</td>
<td>eng1</td>
</tr>
<tr>
<td>vs1.example.com</td>
<td>v1p1</td>
<td>-</td>
<td>off</td>
<td>eng2</td>
</tr>
<tr>
<td>vs1.example.com</td>
<td>v1p2</td>
<td>-</td>
<td>off</td>
<td>native</td>
</tr>
<tr>
<td>vs1.example.com</td>
<td>v1p3</td>
<td>-</td>
<td>off</td>
<td>native</td>
</tr>
<tr>
<td>vs1.example.com</td>
<td>cserver_policy</td>
<td>-</td>
<td>off</td>
<td>eng1</td>
</tr>
<tr>
<td>vs2.example.com</td>
<td>v1p1</td>
<td>3</td>
<td>on</td>
<td>native</td>
</tr>
<tr>
<td>vs2.example.com</td>
<td>v1p2</td>
<td>1</td>
<td>on</td>
<td>eng3</td>
</tr>
<tr>
<td>vs2.example.com</td>
<td>cserver_policy</td>
<td>2</td>
<td>on</td>
<td>eng1</td>
</tr>
</tbody>
</table>
```

**Displaying information about enabled FPolicy policies**

You can display information about enabled FPolicy policies to determine what FPolicy external engine it is configured to use, what the priority is for the policy, and to which Storage Virtual Machine (SVM) the FPolicy policy is associated.

**About this task**

If you do not specify any parameters, the command displays the following information:

- SVM name
- Policy name
• Policy priority

You can use command parameters to filter the command’s output by specified criteria.

**Step**

1. Display information about enabled FPolicy policies by using the appropriate command:

<table>
<thead>
<tr>
<th>If you want to display information about enabled policies...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>On the cluster</td>
<td><code>vserver fpolicy show-enabled</code></td>
</tr>
<tr>
<td>On a specified SVM</td>
<td><code>vserver fpolicy show-enabled -vserver vserver_name</code></td>
</tr>
<tr>
<td>With the specified policy name</td>
<td><code>vserver fpolicy show-enabled -policy-name policy_name</code></td>
</tr>
<tr>
<td>With the specified sequence number</td>
<td><code>vserver fpolicy show-enabled -priority integer</code></td>
</tr>
</tbody>
</table>

The following example displays the information about enabled FPolicy policies on the cluster:

```
cluster1::> vserver fpolicy show-enabled
Vserver               Policy Name       Priority
----------------------- ------------------------- ----------
vs1.example.com         pol_native                native
vs1.example.com         pol_native2               native
vs1.example.com         pol1                      2
vs1.example.com         pol2                      4
```

### Managing FPolicy server connections

You can manage your FPolicy server connections by connecting to external FPolicy servers, disconnecting from external FPolicy servers, or displaying information about connections and connection status.

**Related concepts**

- *What the two parts of the FPolicy solution are* on page 453
- *What synchronous and asynchronous notifications are* on page 453
- *How FPolicy works with external FPolicy servers* on page 455
- *What the node-to-external FPolicy server communication process is* on page 456

### Connecting to external FPolicy servers

To enable file processing, you might need to manually connect to an external FPolicy server if the connection has previously been terminated. A connection is terminated after the server timeout is reached or due to some error. Alternatively, the administrator might manually terminate a connection.

**About this task**

If a fatal error occurs, the connection to the FPolicy server can be terminated. After resolving the issue that caused the fatal error, you must manually reconnect to the FPolicy server.
Steps

1. Connect to the external FPolicy server by using the `vserver fpolicy engine-connect` command.
   For more information about the command, see the man pages.

2. Verify that the external FPolicy server is connected by using the `vserver fpolicy show-engine` command.
   For more information about the command, see the man pages.

Disconnecting from external FPolicy servers

You might need to manually disconnect from an external FPolicy server. This might be desirable if the FPolicy server has issues with notification request processing or if you need to perform maintenance on the FPolicy server.

Steps

1. Disconnect from the external FPolicy server by using the `vserver fpolicy engine-disconnect` command.
   For more information about the command, see the man pages.

2. Verify that the external FPolicy server is disconnected by using the `vserver fpolicy show-engine` command.
   For more information about the command, see the man pages.

Displaying information about connections to external FPolicy servers

You can display status information about connections to external FPolicy servers (FPolicy servers) for the cluster or for a specified Storage Virtual Machine (SVM). This information can help you determine which FPolicy servers are connected.

About this task

If you do not specify any parameters, the command displays the following information:

- SVM name
- Node name
- FPolicy policy name
- FPolicy server IP address
- FPolicy server status
- FPolicy server type

In addition to displaying information about FPolicy connections on the cluster or a specific SVM, you can use command parameters to filter the command's output by other criteria.

You can specify the `-instance` parameter to display detailed information about listed policies. Alternatively, you can use the `-fields` parameter to display only the indicated fields in the command output. You can enter `?` after the `-fields` parameter to find out which fields you can use.

Step

1. Display filtered information about connection status between the node and the FPolicy server by using the appropriate command:
If you want to display connection status information about FPolicy servers...

Enter...

That you specify

vserver fpolicy show-engine -server IP_address

For a specified SVM

vserver fpolicy show-engine -vserver vserver_name

That are attached with a specified policy

vserver fpolicy show-engine -policy-name policy_name

With the server status that you specify

vserver fpolicy show-engine -server-status status

The server status can be one of the following:

• connected
• disconnected
• connecting
• disconnecting

With the specified type

vserver fpolicy show-engine -server-type type

The FPolicy server type can be one of the following:

• primary
• secondary

That were disconnected with the specified reason

vserver fpolicy show-engine -disconnect-reason text

Disconnect can be due to multiple reasons. The following are common reasons for disconnect:

• Disconnect command received from CLI.
• Error encountered while parsing notification response from FPolicy server.
• FPolicy Handshake failed.
• SSL handshake failed.
• TCP Connection to FPolicy server failed.
• The screen response message received from the FPolicy server is not valid.

This example displays information about external engine connections to FPolicy servers on SVM vs1.example.com:

```
cluster1::> vserver fpolicy show-engine -vserver vs1.example.com
FPolicy   Server-   Server-
Vserver         Policy    Node         Server        status        type
--------------- --------- ------------ ------------- ------------- ---------
vs1.example.com policy1  node1        10.1.1.2      connected     primary
vs1.example.com policy1  node1        10.1.1.3      disconnected  primary
vs1.example.com policy1  node2        10.1.1.2      connected     primary
vs1.example.com policy1  node2        10.1.1.3      disconnected  primary
```

This example displays information only about connected FPolicy servers:
cluster1::> vserver fpolicy show-engine -fields server -server-status
connected
node       vserver         policy-name server
---------- --------------- ----------- -------
node1      vs1.example.com policy1     10.1.1.2
node2      vs1.example.com policy1     10.1.1.2

Related concepts

*How FPolicy works with external FPolicy servers* on page 455
*What the node-to-external FPolicy server communication process is* on page 456

Related tasks

*Displaying information about the FPolicy passthrough-read connection status* on page 497

Displaying information about the FPolicy passthrough-read connection status

You can display information about FPolicy passthrough-read connection status to external FPolicy servers (FPolicy servers) for the cluster or for a specified Storage Virtual Machine (SVM). This information can help you determine which FPolicy servers have passthrough-read data connections and for which FPolicy servers the passthrough-read connection is disconnected.

About this task

If you do not specify any parameter, the command displays the following information:

- SVM name
- FPolicy policy name
- Node name
- FPolicy server IP address
- FPolicy passthrough-read connection status

In addition to displaying information about FPolicy connections on the cluster or a specific SVM, you can use command parameters to filter the command’s output by other criteria.

You can specify the `-instance` parameter to display detailed information about listed policies. Alternatively, you can use the `-fields` parameter to display only the indicated fields in the command output. You can enter ? after the `-fields` parameter to find out which fields you can use.

Step

1. Display filtered information about connection status between the node and the FPolicy server by using the appropriate command:

<table>
<thead>
<tr>
<th>If you want to display connection status information about...</th>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPolicy passthrough-read connection status for the cluster</td>
<td>vserver fpolicy show-passthrough-read-connection</td>
</tr>
</tbody>
</table>
If you want to display connection status information about...

<table>
<thead>
<tr>
<th>Enter the command...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FPolicy passthrough-read connection status for a specified SVM</strong></td>
</tr>
<tr>
<td><code>vserver fpolicy show-passthrough-read-connection -vserver vserver_name</code></td>
</tr>
<tr>
<td><strong>FPolicy passthrough-read connection status for a specified policy</strong></td>
</tr>
<tr>
<td><code>vserver fpolicy show-passthrough-read-connection -policy-name policy_name</code></td>
</tr>
<tr>
<td><strong>Detailed FPolicy passthrough-read connection status for a specified policy</strong></td>
</tr>
<tr>
<td><code>vserver fpolicy show-passthrough-read-connection -policy-name policy_name -instance</code></td>
</tr>
<tr>
<td><strong>FPolicy passthrough-read connection status for the status that you specify</strong></td>
</tr>
<tr>
<td><code>vserver fpolicy show-passthrough-read-connection -policy-name policy_name -server-status status</code></td>
</tr>
</tbody>
</table>

The server status can be one of the following:

- connected
- disconnected

The following command displays information about passthrough-read connections from all FPolicy servers on the cluster:

```
cluster1::> vserver fpolicy show-passthrough-read-connection
```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Policy Name</th>
<th>Node</th>
<th>FPolicy Server</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs2.example.com</td>
<td>pol_cifs_2</td>
<td>FPolicy-01</td>
<td>2.2.2.2</td>
<td>disconnected</td>
</tr>
<tr>
<td>vs1.example.com</td>
<td>pol_cifs_1</td>
<td>FPolicy-01</td>
<td>1.1.1.1</td>
<td>connected</td>
</tr>
</tbody>
</table>

The following command displays detailed information about passthrough-read connections from FPolicy servers configured in the “pol_cifs_1” policy:

```
cluster1::> vserver fpolicy show-passthrough-read-connection -policy-name pol_cifs_1 -instance
```

- Node: FPolicy-01
- Vserver: vs1.example.com
- Policy: pol_cifs_1
- Server: 1.1.1.1
- Session ID of the Control Channel: 8ce6f052e-2502-11e3-88d4-123478563412
- Server Status: connected
- Time Passthrough Read Channel was Connected: 9/24/2013 10:17:45
- Reason for Passthrough Read Channel Disconnection: none

Related concepts

- *How FPolicy works with external FPolicy servers* on page 455
- *How FPolicy passthrough-read enhances usability for hierarchical storage management* on page 459

Related tasks

- *Displaying information about connections to external FPolicy servers* on page 495
Copyright information

Copyright © 1994–2015 NetApp, Inc. All rights reserved. Printed in the U.S.

No part of this document covered by copyright may be reproduced in any form or by any means—
graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an
electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and
Disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE,
WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY
DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN
ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice.
NetApp assumes no responsibility or liability arising from the use of products described herein,
except as expressly agreed to in writing by NetApp. The use or purchase of this product does not
convey a license under any patent rights, trademark rights, or any other intellectual property rights of
NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents,
or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to
restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer
Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).
Trademark information

NetApp, the NetApp logo, Go Further, Faster, AltaVault, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCenter, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, and WAFL and other names are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web at http://www.netapp.com/us/legal/netapptmlist.aspx.
How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email to doccomments@netapp.com. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

• NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
• Telephone: +1 (408) 822-6000
• Fax: +1 (408) 822-4501
• Support telephone: +1 (888) 463-8277
Index

8.3-format
  how clustered Data ONTAP uses when creating file and directory names 145

A
  absolute symbolic links
    creating for SMB shares 335
  access
    role authentication plays for SMB 22
  access checks
    security trace, types monitored 284
  access control entries
    See ACEs
  access control lists
    See ACLs
  access restrictions
    configuring for CIFS anonymous (null) users 74
  access tokens
    user, how they are constructed 214
  access-based enumeration
    enabling or disabling from Windows clients 372
    enabling or disabling on SMB shares 371
    introduction to providing folder security on shares with 370
  accounts
    changing or resetting domain passwords for CIFS server 128
  ACEs
    adding to security descriptor DACLs 259
    adding to security descriptor SACLs 271
    defined 253
    managing on resources that contain Dynamic Access Control ACEs when Dynamic Access Control is disabled 200
  ACLs
    advantages of using NTFS, for presentation of UNIX security-style data to SMB clients 75
    commands for managing SMB 190
    creating on SMB shares 188
    default when creating SMB shares 172
    defined 253
    how Data ONTAP uses share-level 188
    introduction to managing SMB share-level 187
    managing on resources that contain Dynamic Access Control ACEs when Dynamic Access Control is disabled 200
  Active Directory
    computer accounts, configuring and managing on SVMs (no CIFS license) 26
    computer accounts, displaying information about discovered LDAP servers and domain controllers for 32
    computer accounts, displaying information about preferred domain controllers for 35
    computer accounts, how to choose whether to create instead of a CIFS server 26, 36
    computer accounts, introduction to managing 27
    computer accounts, introduction to managing domain controller connections for 32
    computer accounts, resetting and rediscovering LDAP servers and domain controllers for 33
    creating computer accounts (no CIFS license) 27
    deleting computer accounts for SVMs 30
    displaying details about restricted group GPOs 123
    displaying information about central access policy rules defined in 125
    displaying information about central access policy rules defined in 126
    displaying information about GPO configurations defined in 120
    joining SVMs to domain 139
  AD
    See Active Directory

  adding
    CIFS server preferred domain controllers 131
    DACL ACEs to a security descriptor 259
    home directory search paths 322
    home directory shares 320
    NetBIOS aliases for CIFS servers, command for 140
    preferred domain controllers for Active Directory
      computer accounts 34
      preferred domain controllers, command for 132
    preferred trusted domains used for multidomain name mapping searches 170
    privileges to local or domain groups 234
    privileges to local or domain users 234
    SACL ACEs to a security descriptor 271
SeSecurityPrivilege privilege to the SQL Server installer's user account 402
shares properties on existing SMB shares 183
shares properties to existing SMB shares, command for 186
tasks to security policies 262, 275
the BranchCache SMB share property 344
users to local groups 230
admin$ default share
what it is and how it is used 173
administrative shares
what the defaults shares are 173
administrator accounts
considerations when using local 217
administrators group, Windows mapping to root 101
AES encryption
enabling or disabling on CIFS servers to configure strong security for Kerberos communications 84
how to use on CIFS servers to configure strong security for Kerberos communications 83
aggregates
space considerations when staging volumes are created by enabled auditing subsystem 424
aliases
determining whether clients are connected using NetBIOS 135
determining which clients are connected using a particular NetBIOS 135
displaying list of NetBIOS, on CIFS servers 134
NetBIOS, introduction to managing on the CIFS server 132
alternate data streams
considerations when auditing files with NTFS 429
anonymous users
configuring access restrictions for CIFS 74
applied security
verifying file and folder 266
applying
audit policies to NTFS files and folders, tasks for 268
file security to NTFS files and folders, tasks for 255
architectures
typical NAS namespace 16
assign
local privileges, how to 217
asynchronous
FPolicy applications 454
FPolicy notifications, defined 453
audit event logs
manually rotating 447
audit policies
adding tasks to 262, 275
configuring using the Windows Security tab 439
creating 261, 274
displaying using the Windows Security tab 443
introduction to configuring file and folder 439
introduction to displaying information about, on FlexVol volumes 240
monitoring jobs 266, 279
NTFS, how to configure using the Data ONTAP CLI 442
tasks for configuring and applying on NTFS files and folders 268
using the Data ONTAP CLI to display information about NTFS 248, 445
verifying applied 279
audit-enabled SVMs
actions you must take before revert 451
auditing
actions you must take on audit-enabled SVMs before revert 451
actions you must take prior to revert 451
aggregate space considerations when enabling 424
commands for modifying configuration 449
configuring for NFS 443
considerations for files with NTFS alternate data streams 429
considerations for symlinks and hard links 429
creating configuration for file and directory events 436
creating file and directory, configuration 436
deleting configuration 450
determining what the complete path to the audited object is 428
displaying information about configuration 448
displaying information about NFSv4, policies 250
displaying information about NTFS audit policies using the Data ONTAP CLI 248, 445
displaying information about volumes or qtrees with Storage-Level Access Guard 158
displaying statistics 305
enabling and disabling on SVMs 447
enabling on the SVM 438
event log consolidation 422
event log consolidation when a node is unavailable 422
event log rotation 422
how active audit logs are viewed using Event Viewer 426
how staging volumes are created on aggregates 424
how the Data ONTAP process works 422
how to troubleshoot event log volume space issues 451
how to troubleshoot staging volume space issues 452
introduction to NFS and SMB file and folder access 421
list of NFS events 431
manually converting the audit event logs 447
partial event log consolidation 422
planning the configuration 431
process when enabling or disabling 422
requirements and considerations for configuring 424
revert process when there are audit-enabled SVMs 451
SMB events that can be audited 426
staging files, staging volumes, consolidation tasks, conversion tasks, defined 421
statistics, determining which counters and objects are available 303, 407
supported audit event log formats 425
verifying applied policies 279
verifying configuration 438
verifying that it is enabled 448
viewing audit event logs 425
authentication
   additional information when using FPolicy external engine connections with SSL 469
   Kerberos 22
   local user, how it works 214
   NTLM 23
   role it plays in securing SMB access 22
   support for Kerberos and NTLM 22
   using local users and groups for 212
authentication security levels
   setting CIFS server minimum 83
   setting LMCompatibilityLevel 83
authorization
   using local users and groups for 212
automatic caching
   configuring BranchCache to provide, for all SMB shares 340
automatic node referrals
   considerations and requirements when using SMB 365
   enabling or disabling SMB 368
   how client response time is improved by SMB 364
   how to monitor using a Windows client 370
   support for SMB 367
   using statistics counters to monitor SMB 368
   verifying that they are disabled for Hyper-V and SQL Server over SMB configurations 399
B
backups
   enabling or disabling VSS shadow copies for Hyper-v over SMB shares 405
   Remote-VSS enabled, considerations when using with Hyper-V over SMB configurations 388
   use remote VSS to perform share-based backups 378
basic concepts
   introduction to how Data ONTAP secures LDAP communication using LDAP over SSL/TLS 95
best practices
   FPolicy setup 462
bits
   how Data ONTAP treats read-only 294
BranchCache
   about using to cache SMB shares at branch offices 336
   changing the server key 348
   configuration prerequisites 339
   configuration recommendations 339
   configuring on CIFS servers 340
   considerations when choosing hash store location 338
   Data ONTAP version requirements 337
   disabling on single SMB shares 355
   displaying hash statistics 305
   displaying information about configurations 347
   displaying information about defined and applied GPOs 353
   displaying statistics 351
   enabling on existing SMB shares 344
   enabling or disabling 357
   enabling when creating SMB shares 343
   flushing hashes from the hash store 350
   GPO support 353
   increasing volume size for hash store directory 346
   information about disabling or enabling 356
   information about how to delete configurations 358
   introduction to enabling on SMB shares 343
   introduction to requirements, considerations, and recommendations for configuring 337
   modifying hash store directory path 346
   modifying hash store maximum directory size 346
   modifying operating mode 346
   modifying the configuration 346
   modifying version support 346
   network protocol support requirements 337
   overview of disabling on SMB shares 354
   pre-computing hashes 349
   share property 344
   stopping automatic caching on all SMB shares 356
   supported SMB 2.1 functionality 104
   versions supported 337
   what happens when reverting 359
   what happens when you delete the configuration 358
   what happens when you disable 356
   where to find information about remote office configuration 343
   Windows hosts version requirements 337
BranchCache hashes
   reasons Data ONTAP invalidates 338
   statistics, determining which counters and objects are available 303, 407
breaking
   locks 297
broadcast domain
   for CIFS server setup, determining which ports are available to add to the new 53
   information to gather before creating CIFS servers 39
broadcast domains
   creating for the IPspace containing the SVM on which the CIFS server is to reside 56
   creating for the IPspace containing the SVM on which the CIFS server will reside 57
   existing, removing ports prior to adding them to the new broadcast domain for CIFS server setup 55
BUILTIN groups
   considerations when using 217
   predefined local 218
bypass traverse checking
   allowing, by adding the SeChangeNotifyPrivilege privilege 239
   information about configuring 237
C
  c$ default share
    what it is and how it is used 173
CA certificates
    converting copy of self-signed root to ASCII text 98
    exporting copy of self-signed root 98
    installing self-signed root, on the SVM 98
CA shares 376
   See also continuously available shares
  caches
    configuring lifetime of SMB metadata 293
disabling automatic computer account password changes 129
displaying details about restricted GPOs applied on 123
displaying information about applied GPO configurations 120
displaying information about central access policies applied on 125
displaying information about central access policy rules applied on 126
displaying information about defined and applied BranchCache GPOs 353
displaying information about discovered LDAP and domain controller servers 130
displaying list of NetBIOS aliases on 134
displaying security setting information 79
enabling LDAP over SSL/TLS on 97
enabling or disabling AES encryption for strong security with Kerberos communication 84
enabling or disabling automatic node referrals 368
enabling or disabling GPO support on 118
enabling or disabling local user authentication for SMB access 220
enabling or disabling local users and groups 219
enabling or disabling ODX 364
enabling or disabling required SMB encryption for incoming SMB traffic on 93
enabling or disabling required SMB signing 88
enabling or disabling VSS shadow copies 405
how export policies for SMB access are handled after Data ONTAP upgrade 206
how GPOs are updated on 119
how SMB signing policies affect SMB communication 85
how they use IPv6 connections to external servers 143
how to choose whether to create, instead of an Active Directory computer account 26, 36
how to use AES encryption to configure strong security for Kerberos communication 83
how to use SMB encryption to enhance security for data transfers over SMB 92
important considerations about security settings in SVM disaster recovery configurations 79
information to gather before creating 39, 49
information to gather before creating the SVM for 42
information to gather for configuring name mappings on 163
information to gather for creating data LIFs on the SVM for 44
introduction to changing computer account passwords for 128
introduction to configuring 36
introduction to configuring default user mappings 99
introduction to configuring SMB on your 103
introduction to creating name mappings on 163
introduction to managing 70
introduction to managing miscellaneous tasks 135
introduction to managing NetBIOS aliases on 132
introduction to managing security settings on 79
IPv6 requirements 141
joining SVMs to an Active Directory domain 139
list of options 70
managing whether to automatically advertise DFS capabilities on 78, 333
manually updating GPO settings on 120
modifying Kerberos security settings 81
moving to different OUs 137
multidomain name mapping searches, configuring preferred trusted domain lists 170
multidomain name mapping searches, displaying information about discovered trusted domains 170
multidomain name mapping searches, displaying information about preferred trusted domain lists 171
multidomain name mapping searches, enabling or disabling on 168
multidomain name mapping searches, rediscovering trusted domains 169
overview of configuration planning 38
prerequisites for setting up 37
removing all NetBIOS aliases from the list on 133
removing NetBIOS aliases from the list on 133
requirements for Hyper-V over SMB 384
requirements for SQL Server over SMB 385
resetting and rediscovering LDAP servers and domain controller servers 130
setting LMCompatibilityLevel 83
setting minimum authentication security level 83
setups, removing ports from existing broadcast domains prior to adding them to the new broadcast domain for 55
SMB share naming considerations 174
stopping or starting 136
supported and unsupported Dynamic Access Control functionality 198
supported GPOs on 113
tasks to configuring LDAP over SSL/TLS on 97
use remote VSS for share-based backups of virtual machines 378
using local users and groups for authentication and authorization 212
using options to customize 70
using privileges to manage access to resources 212
using statistics counters to monitor SMB automatic node referral activity 368
verifying option settings for Hyper-V and SQL Server over SMB configurations 398
what happens to local users and groups when deleting 215
what happens to SMB shares when deleting 172
CIFS services
IPv6 network supported for communication with 141
IPv6 support with 142
CIFS sessions
See SMB sessions
CIFS setups
determining which ports are available to add to the new broadcast domain for 53
CIFS-NDO subsystems
displaying health monitor configuration information for 411
client access failures
how to troubleshoot staging volume space issues that result in 452
clients
requirements for using folder redirection on Windows 313
requirements for using roaming profiles on Windows 311
SMB, supported 37
clusters that support Previous Versions 315
role with FPolicy implementations 454
commands for enabling or disabling oplocks on volumes or qtrees 110
for managing name mappings 166
for managing NTFS DACL ACEs 281
for managing NTFS SACL ACEs 281
for managing NTFS security descriptors 281
for managing search paths 328
for managing security policies 282
for managing security policy jobs 282
for managing security policy tasks 282
for modifying SVM auditing configurations 449
comments how to send feedback about documentation 501
components differences between Data ONTAP and Windows handling of locks on share path 295
calendar account passwords configuring automatic changing of, on CIFS servers 128
disabling automatic changing of, for CIFS servers 129
introduction to changing CIFS server 128
calendar accounts Active Directory, configuring and managing on SVMs (no CIFS license) 26
Active Directory, how to choose whether to create instead of a CIFS server 26, 36
Active Directory, introduction to managing 27
adding or removing preferred domain controllers for Active Directory 34
changing Active Directory domains that SVMs are associated with 28
changing or resetting passwords for CIFS server 128
creating Active Directory (no CIFS license) 27
deleting Active Directory, for SVMs 30
displaying information about discovered LDAP servers and domain controllers for Active Directory 32
displaying information about preferred domain controllers for Active Directory 35
for SVMs, changing or resetting passwords for Active Directory 31
for SVMs, displaying information about Active Directory 30
introduction to managing domain controller connections for Active Directory 32
resetting and rediscovering LDAP servers and domain controllers for Active Directory 33
verifying mapping to default UNIX user for Hyper-V over SMB solutions 395
Computer Management MMC using to configure offline files support on shares 310
concepts introduction to how Data ONTAP secures LDAP communication using LDAP over SSL/TLS 95
nondisruptive operations for Hyper-V and SQL Server over SMB 374
Remote VSS, defined 378
configuration requirements LIF file access management 19
configuration types FPolicy, defined 458
configuration workflows Storage-Level Access Guard 153
configuration, subnet information to gather before creating CIFS servers 39
configurations home directories, additional 328
planning auditing 431
configuring Active Directory computer accounts on SVMs (no CIFS license) 26
advanced NTFS file and folder permissions using the Windows Security tab 192
audit policies on NTFS files and folders, tasks for 268
audit policies using the Windows Security tab 439
auditing for file and directory events 436
auditing for NIS 443
BranchCache on CIFS servers 340
CIFS server options 70, 74
CIFS servers, introduction to 36
default UNIX user 99
DNS services on the SVM 63
dynamic DNS on the SVM 64
file security on NTFS files and folders, tasks for 255
folder redirection 313
FPolicy 485
home directories using %u 325
home directories using %w and %d 323
LDAP over SSL/TLS, tasks to 97
lifetime of SMB metadata cache entries 293
NIS or LDAP name services on the SVM 67
NTFS file permissions using the Data ONTAP CLI, how to 195
offline files support on shares using the Computer Management MMC 310
offline files support on SMB shares 309
roaming profiles 312
security style on FlexVol volumes 147
security style on qtrees 147
security style on SVM root volumes 147
SMB share access control lists 188
standard NTFS file permissions using Windows Security tab 190
time services prior to creating CIFS servers 52
UNIX symbolic link support on SMB shares 334
VSS shadow copy directory depth 402
connecting to external FPolicy servers 494
connection credentials FPolicy, how used with privileged data access channels 455
collections
additional information when using SSL authentication for FPolicy external engine 469
considerations
aggregate space, for staging volumes when enabling auditing 424
auditing configuration 424
for Dynamic Access Control when reverting to a Data ONTAP version that does not support 204
for Remote VSS with Hyper-V over SMB configurations 388
for SMB automatic node referrals 365
for using ODX 362
Hyper-V over SMB configuration 386
revert, when there are local users and groups 215
SMB share naming on CIFS servers 174
SQL Server over SMB configuration 387
when choosing BranchCache hash store location 338
when creating security traces 284
when deploying offline files 308
when modifying security policy jobs 280
when reverting export policies for SMB access 211
when reverting Hyper-V over SMB configurations 406
when using BUILTIN groups and local administrator accounts 217
considerations when applying file-directory policies that use local users or groups on the destination
SVM disaster recovery 79, 254
consolidation tasks
defined for auditing 421
continuously available shares
creating for Hyper-V and SQL Server over SMB configurations 401
creating NTFS data volumes for 400
how they work with Witness to provide transparent failover 376
information to gather when creating for Hyper-V and SQL Server over SMB configurations 391
requirements for Hyper-V over SMB 386
requirements for SQL Server over SMB 387
verifying for Hyper-V and SQL Server over SMB configurations 412
control channels
how FPolicy uses 455
controllers
adding CIFS server preferred domain 131
commands for managing preferred domain 132
conversion tasks
defined for auditing 421
converting
copy of self-signed root CA certificate to ASCII text 98
copy offload
considerations for using ODX 362
how it is used with Hyper-V and SQL Server over SMB configurations 381
how it works 360
use cases for 363
See also ODX
counters
statistics, determining which are available 303, 407
using to monitor SMB automatic node referrals 368
creating
Active Directory computer accounts (no CIFS license 27
auditing configuration for file and directory events 436
BranchCache-enabled SMB shares 343
CIFS servers 65
CIFS servers, command for 140
CIFS servers, introduction to 36
continuously available shares for Hyper-V and SQL Server over SMB configurations 401
Data ONTAP configurations for Hyper-V or SQL Server over SMB, introduction to 393
file and directory auditing configuration 436
FPolicy configurations 485
FPolicy events 487
FPolicy external engines 486
FPolicy policies 487
FPolicy scopes 489
home directory configurations using %u 325
home directory configurations using %w and %d 323
LIFs for CIFS servers 61
local groups 227
local user accounts 221
name mappings 165
NTFS data volumes for continuously available shares 400
security trace filters 286
SMB share access control lists 188
SMB shares on CIFS server 177
SMB shares with the force-group setting 182
SMB shares, command for 186
SMB shares, information needed when 176
SVM for hosting CIFS server 59
symbolic link mappings for SMB shares 335

D

DAC
See Dynamic Access Control
DACLs
adding ACEs to security descriptors 259
commands for managing ACEs in NTFS 281
defined 253
See also NTFS file permissions
See also NTFS file permissions
data access
introduction to how security styles affect 20
data access channels
how FPolicy connection credentials are used with privileged 455
how FPolicy uses privileged 455
data LIFs
considerations when modifying required SMB signing with multiple 87
how control channels are used with FPolicy communication 455
how FPolicy handle migrations and failovers for 457
requirements for Hyper-V and SQL Server over SMB configurations 383
role with FPolicy implementations 454
Data ONTAP
differences with Windows handling of locks on share path components 295
how export policies for SMB access are handled after upgrades 206
how the auditing process works 422
local users and groups 212
requirements for Hyper-V and SQL Server over SMB configurations 383
requirements for using Previous Versions 315
understanding SMB file access with 15
Data ONTAP CLI
how to configure NTFS audit policies using 442
data streams
considerations when auditing files with NTFS alternate 429
data volumes
NTFS, creating for continuously available shares 400
DDNS
See dynamic DNS
default administrative shares
what they are 173
default privileges
predefined BUILTIN group 218
default UNIX user
verifying that Hyper-V and SQL Server domain accounts map to the 395
default UNIX users
configuring 99
definitions
FPolicy 453
local privileges 216
local users and groups 212
SMB shares 172
deleting
Active Directory computer accounts for SVMs 30
all security trace records 292
audit configuration 450
BranchCache configuration, what happens when you 358
CIFS servers, command for 140
local groups 231
local user accounts 226
name mappings, command for 166
security trace filters 290
security trace records 291
SMB shares, command for 186
DFS advertisements
automatic, how to control in clustered Data ONTAP
with a CIFS server option 77, 332
managing whether the CIFS server provides automatic 78, 333
directories
displaying information about a specified user's home
directory path 329
home, unique user names required for share 322
directory events
creating auditing configuration for 436
directory names
case-sensitivity in a multiprotocol environment 145
case-sensitivity when creating shares in a multiprotocol environment 175
dependencies for NFS and SMB 145
how clustered Data ONTAP creates 145
valid characters for 145
directory structures
used by Remote VSS, example of 379
directory traverse checking
disallowing users and groups from bypassing 240
disabling
access-based enumeration on SMB shares 371
AES encryption on CIFS servers to configure strong security for Kerberos communications 84
auditing on SVMs 447
BranchCache 357
BranchCache, what happens when you 356
Dynamic Access Control 199
export policies for SMB access 207
FPolicy policies 491
GPO support 118
local user accounts 223, 224
local user authentication for SMB access 220
local users and groups 219
multidomain name mapping searches 168
ODX 364
required password complexity for local users 80
required SMB encryption for incoming SMB traffic on CIFS servers 93
required SMB signing 88
SMB 2.x on SVMs with FlexVol volumes 106
SMB 3.0 on SVMs with FlexVol volumes 107
SMB automatic node referrals 368
the Windows guest user account 100
VSS shadow copies 405
disaster recovery
for SVMs, important considerations about CIFS server security settings in configurations for 79
security certificates for FPolicy do not replicate in SVM non-ID-preserve configurations 469
disconnecting
from external FPolicy servers 495
discovered trusted domains
displaying information about 170
discretionary access control lists 190
See also NTFS file permissions
displaying
audit policy information on FlexVol volumes, introduction to 240
audit policy information using the Windows Security tab 443
auditing statistics 305
BranchCache hash statistics 305
BranchCache statistics 351
central access policies applied to CIFS servers and defined in Active Directory 125
central access policy rules applied to CIFS servers and defined in Active Directory 126
CIFS and SMB statistics 305
CIFS server security setting information 79
CIFS servers, command for 140
continuously available protection information 298, 415
details about restricted group GPOs applied to CIFS server and defined in Active Directory 123
Dynamic Access Control security information on NTFS and mixed security-style volumes 203
file security information for NTFS security-style volumes 242
file security information on mixed security-style volumes 244
file security information on UNIX security-style volumes 246
file security information, introduction to 240
FPolicy configuration information, commands for 492
FPolicy configuration, how show commands work when 492
group membership for local users 225
health monitor status for Hyper-V over SMB 411
health monitor status for SQL Server over SMB 411
information about a user's home directory path 329
information about active Directory computer accounts for SVMs 30
information about auditing configurations 448
information about BranchCache configurations 347
information about connections to external FPolicy servers 495
information about defined and applied BranchCache GPOs 353
information about discovered active Directory LDAP servers and domain controllers 32
information about discovered LDAP and domain controller servers 130
information about discovered trusted domains 170
information about enabled FPolicy policies 493
information about FPolicy configurations 491
information about FPolicy passthrough-read connection status 497
information about FPolicy policy status 492
information about GPO configurations applied to CIFS server and defined in Active Directory 120
information about local groups 229
information about local user accounts 225
information about locks 295
information about preferred domain controllers for Active Directory computer accounts 35
information about SMB open files 298
information about SMB sessions 298
information about SMB statistics 298
information about the list of preferred trusted domains 171
information about the ordering of discovered trusted domains 170
information about user types connected over SMB sessions 102
IPv6 SMB session information 144
members of local groups 231
name mappings, command for 166
NetBIOS over TCP information 140
NFSv4 audit information on FlexVol volumes 250
NTFS auditing information on FlexVol volumes using the Data ONTAP CLI 248, 445
preferred domain controllers, command for 132
privilege overrides 237
security trace filters 287
security trace results 288
shares properties for existing SMB shares, command for 186
SMB open file information 301, 418
SMB session information 298, 415
SMB session open file information 301, 418
SMB shares, command for 186
SMB statistics 409
Storage-Level Access Guard file security information for volumes or qtrees 158
traditional and lease oplock status 111
volume mount and junction point information 151
DNS
information to gather for configuring 45
services, configuring on the SVM 63
documentation
how to receive automatic notification of changes to 501
how to send feedback about 501
domain accounts
changing or resetting passwords for CIFS server 128
verifying mapping to default UNIX user for SQL Server over SMB solutions 395
domain controller connections
for active directory computer accounts, introduction to managing 32
domain controllers
adding or removing preferred, for active directory computer accounts 34
adding preferred 131
commands for managing preferred 132
displaying information about discovered 130
displaying information about discovered active directory 32
displaying information about preferred, for active directory computer accounts 35
resetting and rediscovering Active Directory 33
SMB, supported 37
domain, broadcast
information to gather before creating CIFS servers 39
domains
adding, removing, or replacing trusted domains from the list of preferred trusted 170
displaying information about discovered trusted 170
displaying information about the list of preferred trusted 171
joining SVMs to Active Directory 139
rediscovering trusted, used for multidomain name mapping searches 169
durable handles
supported SMB 2.0 functionality 103
supported SMB 2.1 functionality 104
Dynamic Access Control
configuring central access policies 200
considerations when reverting to a Data ONTAP version that does not support 204
considerations when using with CIFS server objects 199
enabling or disabling 199
introduction to securing SMB access using 196
managing ACLs that contain Dynamic Access Control ACEs when disabled 200
security on mixed volumes, displaying information about 203
security on NTFS volumes, displaying information about 203
supported and unsupported functionality 198
where to find additional information for configuring and using 204
dynamic DNS
  configuring on the SVM 64
  modifying on the SVM before moving the CIFS server to another domain 138

E
effective security styles
  UNIX, how UNIX file permissions provide access control over SMB 196
enabling
  access-based enumeration on SMB shares 371
  AES encryption on CIFS servers to configure strong security for Kerberos communications 84
  auditing on SVMs 447
  auditing on the SVM 438
  BranchCache 357
  BranchCache automatic caching on all SMB shares 340
  Dynamic Access Control 199
export policies for SMB access 207
FPolicy policies 489, 491
GPO support 118
IPv6 on the cluster for SMB 144
LDAP over SSL/TLS on the CIFS server 97
local user accounts 223, 224
local user authentication for SMB access 220
local users and groups 219
multidomain name mapping searches 168
ODX 364
required password complexity for local users 80
required SMB encryption for incoming SMB traffic on CIFS servers 93
required SMB signing 88
SMB 2.x on SVMs with FlexVol volumes 106
SMB 3.0 on SVMs with FlexVol volumes 107
SMB automatic node referrals 368
SMB metadata caches 293
the Windows guest user account 100
VSS shadow copies 405
encrypted SMB sessions
determining whether clients are connected using 94
enumeration
  access-based, enabling or disabling from Windows clients 372
error messages
  No space left on device 452
event log formats
  support for EVTIX file format 425
  support for XML file format 425
event logs
  manually rotating audit 447
  supported file formats for audit 425
  viewing audit 425
Event Viewer
  how active audit logs are viewed using 426
  events
    command for displaying information about FPolicy 492
    command for modifying FPolicy 490
creating auditing configuration for file and directory 436
creating FPolicy 487
information to gather for configuring FPolicy 477
planning the configuration for FPolicy 472
SMB, that can be audited 426
supported combinations of file operations and filters that FPolicy can monitor for NFSv3 476
supported combinations of file operations and filters that FPolicy can monitor for NFSv4 476
supported combinations of file operations and filters that FPolicy can monitor for SMB 475

EVTX
  file format, viewing audit event logs with 425
  supported audit event log file format 425
exchanging
  name mappings, command for 166
export policies
  considerations when reverting for SMB access 211
  enabling or disabling for SMB access 207
  examples of rules for SMB access 209
  for SMB access, how handled after Data ONTAP upgrade 206
  how used with SMB access 205
  introduction to securing SMB access using 205
  role in SMB access 24
export rules
  how they work 208
export-level security
  how used to secure access 24
exporting
  copy of self-signed root CA certificate 98
external communication
  how FPolicy handles during node failover 457
external engines
  command for displaying information about FPolicy 492
  command for modifying FPolicy 490
  creating FPolicy 486
  information to gather for configuring FPolicy 470
  planning the configuration for FPolicy 464
external FPolicy servers
  configuration type defined 458
  connecting to 494
  disconnecting from 495
  displaying information about connections to 495
  how FPolicy works with external FPolicy servers 455
  when to create FPolicy configurations that use 459
external servers
  how CIFS servers use IPv6 when connecting to 143

F
failover
  how FPolicy handles external communication during node 457
failures
  how to troubleshoot staging volume space issues that result in client access 452
features
  unsupported Windows 37
feedback
how to send comments about documentation 501
file access
LIF configuration requirements for managing 19
file access events
using FPolicy to monitor 453
file and directory auditing
creating configuration on SVMs 436
file and folder access
how three levels of security used to secure 24
introduction to auditing NFS and SMB 421
file and folder access events
SMB, that can be audited 426
file and folder security
how security descriptors are used 253
limits for using the CLI to set 252
use cases for using the CLI to set 252
file audit policies
introduction to configuring 439
file caching
introduction to using offline files for offline use 307
file events
creating auditing configuration for 436
file formats
viewing audit event logs with XML or EVTX 425
file locking
between protocols, explained 294
file locks
breaking 297
displaying information about 295
introduction to managing 294
file name translations
commands for managing NFS to SMB character mapping for 163
configuring character mapping for SMB on FlexVol volumes 161
file names
case-sensitivity in a multiprotocol environment 145
dependencies for NFS and SMB 145
how clustered Data ONTAP creates 145
valid characters for 145
file operations
displaying security trace results for 288
supported combinations of file operations and filters for NFSv4 FPolicy events 476
supported combinations of file operations and filters for SMB FPolicy events 475
supported combinations with filters for NFSv3 FPolicy events 476
file permissions
effect of security styles on 20
how to configure NTFS, using the Data ONTAP CLI 195
introduction to securing SMB access using 190
NTFS, configuring advanced file and folder permissions using the Windows Security tab 192
NTFS, configuring standard file and folder permissions using the Windows Security tab 190
UNIX, when used to provide access control over SMB 196
file security
creating NTFS security descriptors 257, 269
displaying for mixed security-style volumes 244
displaying for UNIX security-style volumes 246
displaying information about volumes or qtrees with Storage-Level Access Guard 158
information, displaying for NTFS security-style volumes 242
introduction to displaying information about 240
tasks for configuring and applying on NTFS files and folders 255
verifying applied 266
file security policies
adding tasks to 262, 275
creating 261, 274
monitoring jobs 266, 279
file-directory policies
considerations for local users and groups when applying to the SVM disaster recovery destination 254
file-level and folder-level security
how used to secure access 24
files
configuring support on SMB shares for offline 309
considerations when deploying offline 308
how to troubleshoot space issues related to volumes that contain staging 452
introduction to using to cache files for offline use 307
requirements for using offline 308
files and folders
configuring advanced NTFS file permissions on, using the Windows Security tab 192
configuring standard NTFS file permissions on, using the Windows Security tab 190
filters
creating security trace 286
displaying security trace 287
supported combinations of file operations and filters for NFSv4 FPolicy events 476
supported combinations of file operations and filters for SMB FPolicy events 475
supported combinations with file operations for NFSv3 FPolicy events 476
FlexVol volumes
commands for managing NFS to SMB character mapping on 163
configuring character mappings for SMB file name translation on 161
configuring security style on 147
folder audit policies
introduction to configuring 439
folder redirection
configuring 313
introduction to using to store data on a CIFS server 312
requirements for using 313
folder security
verifying applied 266
force-group
share setting, what it does 182
force-group setting
creating SMB shares with the 182
FPolicy
how passthrough-read enhances usability for HSM 459
how read requests are managed when passthrough-read is enabled 460
upgrade and revert considerations for passthrough-read 462
FPolicy best practices
for setup 462
FPolicy communications
synchronous and asynchronous notifications, defined 453
FPolicy configuration types
defined 458
when to create a native FPolicy configuration 459
when to create configurations that use external FPolicy servers 459
FPolicy configurations
commands for displaying information about 492
commands for modifying 490
creating 485
displaying information about 491
how show commands work when displaying information about 492
information about requirements, considerations, and best practices 461
overview of configuration planning 464
steps to setup 463
FPolicy connections
displaying information about external server connections 495
how connection credentials are used with privileged data access channels 455
how control channels are used with 455
how data LIF migrations and failovers are handled 457
how privileged data access channels are used 455
management responsibilities when connecting to external FPolicy servers 455
synchronous and asynchronous applications 454
synchronous and asynchronous notifications, defined 453
what it means to grant super user credentials for privileged data access 456
what the node-to-external FPolicy server communication process is 456
FPolicy events
creating 487
information to gather for configuring 477
planning the configuration for 472
supported combinations of file operations and filters for NFSv3 476
supported combinations of file operations and filters for NFSv4 476
supported combinations of file operations and filters that FPolicy can monitor for SMB 475
FPolicy external communication
how managed during node failovers 457
FPolicy external engines
additional information about configuring SSL authenticated connections for 469
creating 486
information to gather for configuring 470
planning the configuration for 464
security certificates for SSL authentication with FPolicy do not replicate in SVM non-ID-preserve configurations 469
with MetroCluster and SVM disaster recovery, restrictions when choosing authentication methods for 470
FPolicy external servers
See FPolicy servers
FPolicy framework
defined 453
protocols that can be monitored 453
roles that cluster components play with 454
what it does 453
FPolicy notifications
synchronous and asynchronous, defined 453
FPolicy policies
creating 487
displaying information about enabled 493
displaying information about status 492
enabling 489
enabling or disabling 491
how FPolicy manages processing multiple 456
information to gather for configuration 482
planning the configuration for 477
requirements for FPolicy scopes if using the native engine for 481
FPolicy scopes
configuration information to gather 484
creating 489
planning the configuration for 482
requirements if using the FPolicy policy uses the native engine 481
FPolicy servers
connecting to external 494
disconnecting from external 495
displaying information about connections to external 495
displaying information about FPolicy passthrough-read connection status 497
how FPolicy works with external FPolicy servers 455
what the communication process to nodes is 456
what they do 453
when to create FPolicy configurations that use external 459
FPolicy services
how they work across SVM namespaces 458
FPolicy setup
recommendations for 462
requirements for 461
G

gathering information
for cluster time services setup 38
for configuring name services 45
for creating CIFS servers 49
for creating data LIFs on the SVM 44
for the IPspace, broadcast domain, and subnet configuration 39
for the SVM configuration 42
GPOs
applying to CIFS servers 113
displaying details about restricted groups applied to CIFS server and defined in Active Directory 123
displaying information about central access policies applied to CIFS servers and defined in Active Directory 125
displaying information about central access policy rules applied to CIFS servers and defined in Active Directory 126
displaying information about configurations applied to CIFS server and defined in Active Directory 120
displaying information about defined and applied BranchCache 353
enabling or disabling support for 118
how updated on the CIFS server 119
manually updating settings 120
requirements for using with CIFS servers 118
support for BranchCache 353
supported 113
what to do if updates are failing 119
group memberships
displaying local user 225
Group Policy Objects
See GPOs
groups
adding privileges to local or domain 234
adding users to local 230
considerations when using BUILTIN 217
considerations when using SnapMirror on SVMs with local 215
creating local 227
deleting CIFS servers, what happens to local 215
deleting local 231
disallowing from bypassing directory traverse checking 240
displaying information about local 229
displaying list of members of local 231
how user access tokens are constructed for local 214
modifying description for local 228
predefined local BUILTIN 218
removing privileges from local or domain 235
removing users from local 230
renaming local 228
resetting privileges for local or domain 236
revert considerations when there are local 215
updating names in the local databases for domain 232
groups, Windows administrator
mapping to root 101
guaranteed auditing
how Data ONTAP ensures 422

H
hard links
considerations when auditing 429
hash store directory path
modifying for BranchCache configurations 346
hash store maximum directory size
modifying for BranchCache configurations 346
hash stores
configuring maximum size for BranchCache 340
considerations when choosing location for BranchCache 338
hashes
flushing from the BranchCache hash store 350
pre-computing BranchCache 349
reasons Data ONTAP invalidates BranchCache 338
hierarchical storage management
See HSM
home directories
adding search paths 322
additional configurations 328
creating configurations using %u 325
creating configurations using %w and %d 323
displaying information about a specified user's home directory path 329
enabling or disabling other user access (public access) to user 329
enabling or disabling Windows administrator access to user 329
how clustered Data ONTAP enables dynamic SMB 319
introduction to managing 319
shares require unique user names 322
what happens to static share names after upgrading 322
home directory shares
adding 320
HSM
how FPolicy passthrough-read enhances usability for 459
Hyper-V over SMB
CIFS server requirements when configuring 384
concepts 374
configurations, creating continuously available shares for 401
configurations, information to gather for creating volumes 390
configuring existing shares for continuous availability 403
configuring VSS shadow directory depth 402
considerations when reverting 406
considerations when using Remote VSS-enabled backup solutions with 388
creating NTFS data volumes for continuously available shares 400
Data ONTAP and licensing requirements when configuring 383
enabling or disabling VSS shadow copies for backups over SMB shares 405
example of directory structure used by Remote VSS 379
how ODX copy offload is used with 381
how SMB 3.0 functionality supports 376
how SnapManager for Hyper-V manages Remote VSS-based backups 380
how to use system health monitor to determine nondisruptive operation status 410
information about configuration requirements and considerations 382
information about managing configurations 403
information about using statistics to monitor SMB activity 407
information to gather for creating continuously available SMB shares 391
introduction to configuration planning tasks 390
introduction to creating Data ONTAP configurations for nondisruptive operations with 393
network and data LIF requirements when configuring 383
nondisruptive operations for, defined 373
protocols that provide capabilities for nondisruptive operations 374
recommendations when configuring 389
requirements and considerations when configuring 386
requirements when using ODX copy offload 389
support for stand-alone and clustered configurations 373
supported nondisruptive operations 373
use remote VSS for share-based backups of virtual machines 378
verifying CIFS server option settings for NDOs with 398
verifying continuously available SMB share configuration 412
verifying LIF status 413
verifying that automatic node referrals are disabled 399
verifying that computer accounts map to the default UNIX user 395
verifying that Kerberos and NTLMv2 authentication are permitted 394
verifying that root volume is set to NTFS security style 397
volume requirements when configuring 384
what you need to configure 373

I
ID discard
considerations when applying file-directory policies that use local users or groups on the SVM disaster recovery destination 254
important considerations about CIFS server security settings in configurations for SVM disaster recovery configurations with 79
Infinite Volumes
where to find information about SMB support on 69
where to get information about security styles of 146
information
how to send feedback about improving documentation 501
inserting
name mappings, command for 166
installing
self-signed root CA certificate on the SVM 98
interpreting
security trace results 292
invalidating
BranchCache hashes, reasons for 338
IP spaces
creating broadcast domains for 56
creating broadcast domains for the 57
ipc$ default share
what it is and how it is used 173
IPspaces
creating for the SVM on which the CIFS server will reside 32
determining which ports are available to add to the new broadcast domain 53
information to gather before creating CIFS servers 39
removing ports from existing broadcast domains prior to adding them to new broadcast domains for CIFS server setups 55
IPv6
displaying information about SMB sessions 144
enabling on the cluster for SMB 144
how CIFS servers use, when connecting to external servers 143
how to disable on the cluster 144
monitoring SMB sessions for 144
requirements for SMB 141
support with SMB and CIFS services 142
supported network for SMB access and CIFS services 141
J
jobs
commands for managing security policy 282
considerations when modifying security policy 280
monitoring security policy jobs 266, 279
junction points
creating volumes with specified 148
creating volumes without specified 149
displaying information about volume 151
elimination of execute permission requirement for SMB shares when crossing 175
volume, how used to create namespaces 15
junctions
considerations with Previous Versions restores for folders with 318
defined 15
usage rules 15
volume, how used in SMB and NFS namespaces 16
K
KDC Resource
support for SID Compression 22
Kerberos
authentication 22
communications, enabling or disabling AES encryption on CIFS servers to configure strong security for 84
how export policies are used with SMB access for authentication 205
information to gather for setting up time services for CIFS authentication 38
verifying that authentication is permitted with Hyper-V over SMB configuration 394
Kerberos communication
how to use AES encryption on CIFS servers to configure strong security for 83
Key Distribution Center
See KDC
LDAP
- displaying information about discovered servers 130
- configuring on the SVM 67

LDAP over SSL/TLS
- converting exported copy of self-signed root CA certificate to ASCII text 98
- enabling on the CIFS server 97
- exporting copy of self-signed root CA certificate 98
- installing self-signed root CA certificate on the SVM 98
- introduction to configuring and using to secure communication 95
- introduction to how Data ONTAP uses to secure LDAP communication 95
- tasks to configuring on CIFS servers 97

LDAP servers
- displaying information about discovered Active Directory 32
- resetting and rediscovering Active Directory 33

lease oplocks
- enabling or disabling on existing SMB shares 109
- enabling or disabling when creating SMB shares 108
- improving SMB client performance with 107
- monitoring 111
- supported SMB 2.1 functionality 104

licensing
- requirements for Hyper-V and SQL Server over SMB configurations 383

LIFs
- configuration requirements for file access management 19
- creating for CIFS servers 61
- data, information to gather for creating on the SVM 44
- data, role with FPolicy implementations 454
- how FPolicy handle migrations and failovers for data 457
- requirements for Hyper-V and SQL Server over SMB configurations 383
- verifying status for Hyper-V over SMB configurations 413
- verifying status for SQL Server over SMB configurations 413

limits
- for using the CLI to set file and folder security 252
- when configuring UNIX symbolic links for SMB access 332

link mappings
- creating symbolic, for SMB shares 335

links
- configuring support for UNIX symbolic, on SMB shares 334
- how SMB clients can access UNIX symbolic 331
- limits when configuring UNIX symbolic, for SMB access 332

lists
- of CIFS server options 70
- of supported privileges 216

LMCompatibilityLevel
- setting CIFS server 83

local administrator accounts
- considerations when using 217
- local groups
- considerations when using SnapMirror on SVMs with 215
- creating 227
- deleting 231
- displaying information about 229
- displaying list of members of 231
- predefined BUILTIN 218
- reasons for creating 213
- local links
- how SMB clients can access UNIX symbolic links 331
- local privileges
- defined 216
- how to assign 217
- local user authentication
- enabling or disabling for SMB access 220
- local users
- changing account passwords 224
- deleting accounts 226
- displaying information about 225
- displaying information about local group membership 225
- enabling or disabling accounts 224
- enabling or disabling required password complexity for 80
- how authentication works 214
- modifying, renaming, enabling, or disabling 223
- password requirements 217
- reasons for creating 213
- local users and groups
- defined 212
- deleting CIFS servers, what happens to 215
- enabling or disabling 219
- file-directory policies containing, considerations when applying to the SVM disaster recovery destination 254
- how Data ONTAP uses 212
- how they are used 212
- how user access tokens are constructed 214
- reasons for creating 213
- revert considerations when they are configured 215
- using for authentication and authorization 212
- view from the Microsoft Management Console 215

locks
- breaking 297
- differences between Data ONTAP and Windows handling of, on share path components 295
- displaying information about 295

logon and logoff events
- SMB, that can be audited 426

logs
- manually rotating audit logs 447

M
- managing
- Active Directory computer accounts on SVMs (no CIFS license) 26
- CIFS servers, commands for 140
- file access with SMB shares 212
introduction to, NTFS file security and audit policies using the CLI 251
introduction to, Storage-Level Access Guard using the CLI 251
local group memberships 230
name mappings, commands for 166
preferred domain controllers, commands for 132
SMB share properties, commands for 186
SMB shares, commands for 186
symbolic link mapping, commands for 336
manually rotating audit event logs 447
mapping Windows administrators group to root 101
mappings creating symbolic link, for SMB shares 335
metadata caches configuring lifetime of SMB 293
enabling SMB 293
introduction to configuring for SMB 1.0 shares 293
metadata caching how it works in SMB 293
MetroCluster configurations restrictions when choosing authentication methods for cluster-scoped FPolicy external engines with 470
Microsoft Management Console view information about local users and groups from the 215
what management tasks you can perform on local users and groups 215
See also MMC
Microsoft SQL Server
See SQL Server
Microsoft SQL Server over SMB supported nondisruptive operations 373
minimum authentication security levels setting CIFS server 83
setting LMCompatibilityLevel 83
MMC connecting to the SVM to view SMB shares 186
using to configure offline files support on shares 310
modifying auditing configurations, commands for 449
BranchCache configurations 346
CIFS server Kerberos security settings 81
CIFS servers, command for 140
existing shares for continuous availability 403
FPolicy configurations, commands for 490
local group descriptions 228
local user accounts 223
local user's full name or description 223
name mapping patterns, command for 166
protocols for SVMs 136
security trace filters 289
SMB shares, command for 186
monitoring automatic node referrals using a Windows client 370
SMB activity 298
SMB signing statistics 90
traditional and lease oplocks 111
mounting volumes in NAS namespaces 150
moving CIFS servers to another domain, command for 140
moving CIFS servers modifying dynamic DNS on the SVM before 138
multidomain name mapping searches adding, removing, or replacing trusted domains in preferred trusted domains lists 170
displaying information about discovered trusted domains 170
displaying information about the list of preferred trusted domains 171
enabling or disabling 168
introduction to configuring 166
rediscovering trusted domains used for 169
multidomain searches for name mapping, introduction to configuring 166

N
name mapping how it works 23
name mappings adding, removing, or replacing trusted domains in preferred trusted domains lists 170
conversion rules 164
creating 165
displaying information about discovered trusted domains used for multidomain searches 170
displaying information about the list of preferred trusted domains used for multidomain searches 171
enabling or disabling multidomain searches for 168
for searches, introduction to configuring multidomain 166
how used with SMB access 23
introduction to creating 163
multidomain searches for UNIX user to Windows user 166
rediscovering trusted domains used for multidomain searches 169
verifying that Hyper-V and SQL server domain accounts map to the default UNIX user 395
name services configuring on the SVM 67
information to gather for configuring 45
name services switch information to gather for configuring 45
names how clustered Data ONTAP creates file and directory 145
valid characters for file or directory 145
namespaces defined 15
how FPolicy services work across SVM 458
how they affect SMB access 15
how volume junctions are used for NAS access 16
introduction to creating and managing data volumes in NAS 148
mounting or unmounting volumes within NAS 150
typical architectures for NAS 16
NAS creating volumes with specified junction points 148
creating volumes without specified junction points 149
displaying volume mount and junction point information 151
mounting or unmounting volumes in the namespace 150
typical namespace architectures 16
NAS namespaces
introduction to creating and managing data volumes in 148
native engine
requirements for FPolicy scopes if using in FPolicy policy 481
native FPolicy configurations
when to create 459
native FPolicy servers
configuration type defined 458
NB aliases
See NetBIOS aliases
NDOs
See nondisruptive operations
NetBIOS
over TCP, displaying information 140
NetBIOS aliases
adding or removing for CIFS servers, commands for 140
adding to an existing list on the CIFS server 132
creating a list on the CIFS server 132
determining whether clients are connected using 135
determining which clients are connected using a particular 135
displaying list of, on CIFS servers 134
introduction to managing on the CIFS server 132
removing from the CIFS server alias list 133
networks
requirements for Hyper-V and SQL Server over SMB configurations 383
NFS
configuring auditing 443
events that can be audited 431
file and directory naming dependencies 145
file locking between protocols explained 294
how Data ONTAP treats read-only bits 294
modifying protocols for SVMs 136
NFSv4 audit information, displaying 250
NFS clients
configuring character mappings for SMB file name translations on FlexVol volumes 161
NFS exports
how volume junctions are used with 16
NIS
information to gather for configuring 45
name services, configuring on the SVM 67
no CIFS license
configuring and managing Active Directory computer accounts on SVMs 26
No space left on device error
how to troubleshoot 452
node referrals
considerations and requirements when using SMB automatic 365
how client response time is improved by SMB automatic 364
support for SMB automatic 367
nodes
how FPolicy manages external communication during failovers 457
verifying LIF status for Hyper-V and SQL Server over SMB configurations 413
what the communication process is for FPolicy-enabled non-preserved identities
important considerations about CIFS server security settings in configurations for SVM disaster recovery configurations with 79
nondisruptive operations
adding the SeSecurityPrivilege privilege to the user account used to install SQL Server 402
for Hyper-V and SQL Server over SMB, displaying health monitor status for 411
for Hyper-V and SQL Server over SMB, how SMB functionality supports 376
for Hyper-V over SMB, concepts 374
for SQL Server over SMB, concepts 374
Hyper-V over SMB configuration requirements and considerations for 386
Hyper-V over SMB, CIFS server and volume configuration requirements 384
Hyper-V over SMB, defined 373
Hyper-V over SMB, how to use system health monitor to determine status of 410
introduction to Hyper-V or SQL Server over SMB configuration planning tasks 390
introduction to verifying that the configuration is capable of 410
network and data LIF requirements when configuring Hyper-V and SQL Server over SMB for 383
protocols providing capability for Hyper-V and SQL Server over SMB 374
requirements for Hyper-V and SQL Server over SMB configurations 383
SQL Server over SMB configuration requirements and considerations for 387
SQL Server over SMB, CIFS server and volume configuration requirements 385
SQL Server over SMB, defined 373
SQL Server over SMB, how to use system health monitor to determine status of 410
supported SMB 3.0 functionality 105
verifying CIFS server options for Hyper-V and SQL Server over SMB 398
NT STATUS_DUPLICATE_NAME error
what to do if GPO updates lead to the 119
NTFS
configuring advanced file and folder permissions using the Windows Security tab 192
configuring standard file and folder permissions using the Windows Security tab 190
creating security descriptors 257, 269
DACL ACEs, commands for managing 281
data volumes, creating for continuously available shares 400
displaying file security information for NTFS security-style volumes 242
displaying information about Dynamic Access Control security on mixed volumes 203
file security on mixed volumes, displaying information about 244
how to use the Data ONTAP CLI to configure audit policies for 442
SAACL ACEs, commands for managing 281
security descriptors, commands for managing 281
security style on root volumes, verifying for Hyper-V and SQL Server over SMB configurations 397
NTFS ACLs
advantages of using for presentation of UNIX security-style data to SMB clients 75
NTFS alternate data streams
considerations when auditing files with 429
NTFS file permissions
how to configure using the Data ONTAP CLI 195
NTLM
authentication 23
how export policies are used with SMB access for authentication 205
NTLMv2
verifying that authentication is permitted with Hyper-V over SMB configuration 394
NTP
See time services
null users
configuring access restrictions for CIFS 74
O
objects
statistics, determining which are available 303, 407
ODX
considerations for using 362
enabling or disabling 364
how it is used with Hyper-V and SQL Server over SMB configurations 381
how it works 360
improving remote copy performance with 359
requirements for using 361
tokens 360
use cases for 363
ODX copy offload
requirements when using with Hyper-V over SMB solutions 389
requirements when using with SQL Server over SMB solutions 389
offline files
configuring on a share using the Computer Management MMC 310
configuring on SMB shares 309
considerations when deploying 308
how read requests are handled when FPolicy passthrough-read is enabled 460
introduction to using to cache files for offline use 307
requirements for using 308
Offloaded Data Transfer
See ODX
open files
displaying information about SMB 301, 418
operating mode
modifying for BranchCache configurations 346
oplocks
commands for enabling or disabling for volumes or qtrees 110
enabling or disabling on existing SMB shares 109
enabling or disabling when creating SMB shares 108
improving SMB client performance with 107
monitoring 111
write cache data-loss considerations 108
options
CIFS server, managing whether to automatically advertise DFS capabilities 78, 333
See also CIFS server options
options, CIFS servers
list of available 70
organizational units
See OUs
OUs
moving CIFS servers to different 137
overrides
displaying privilege 237
P
passthrough-read
creating FPolicy policies with 487
displaying information about status of connections for FPolicy 497
FPolicy, how read requests are handled when enabled 460
FPolicy, upgrade and revert considerations for 462
passthrough-reads
for FPolicy, how it enhances usability for HSM 459
password complexity
enabling or disabling requirement for local users 80
passwords
changing CIFS server domain account 128
changing local user account 224
computer account, configuring automatic changing of, on CIFS servers 128
computer account, disabling automatic changing of, for CIFS servers 129
enabling or disabling required complexity for local users 80
for SVMs, changing or resetting Active Directory computer account 31
introduction to changing CIFS server computer account 128
requirements for local users 217
resetting for CIFS server domain account 128
path components
differences between Data ONTAP and Windows handling of locks on share 295
path to hash store
specifying for BranchCache configurations 340
paths
commands for managing search 328
determining for audited objects 428
per-share caching
configuring BranchCache to provide, for SMB shares 340
performance
how SMB automatic node referrals improve client 364
impact on with SMB signing 87
improving remote copy performance with ODX 359
using oplocks to improve SMB client 107
performing
security traces, introduction to 285
permissions
configuring SMB share 188
effect of security styles on file 20
how Data ONTAP preserves UNIX 77
UNIX, how to manage using Windows Security tab 77
planning
auditing configuration 431
FPolicy configuration overview 464
FPolicy event configuration 472
FPolicy external engine configurations 464
FPolicy policy configurations 477
FPolicy scope configurations 482
introduction to tasks for configuring Hyper-V or
SQL Server over SMB for nondisruptive operations 390
the CIFS server configuration, overview of 38
policies
command for displaying information about FPolicy 492
command for modifying FPolicy 490
commands for managing security 282
considerations when reverting export, for SMB access 211
creating security 261, 274
displaying information about enabled FPolicy 493
displaying information about FPolicy policy status 492
enabling FPolicy 489
enabling or disabling FPolicy 491
FPolicy, information to gather for configuration 482
how FPolicy manages processing multiple FPolicy 456
introduction to configuring file and folder audit 439
monitoring jobs, file security and auditing 266, 279
planning the configuration for FPolicy 477
security, applying to SVMs with FlexVol volumes 265, 278
security, commands for managing tasks 282
verifying applied audit 279
ports
removing from existing broadcast domains prior to
adding them to the new broadcast domain for CIFS server setups 55
pre-computing
BranchCache hashes 349
predefined
BUILTIN local groups 218
preferred domain controllers
adding 131
adding or removing for Active Directory computer accounts 34
commands for managing 132
displaying information about, for Active Directory computer accounts 35
preferred trusted domains
adding, removing, or replacing trusted domains from the list of 170
displaying information about the list of 171
how used with multidomain searches for user name mapping 166
prerequisites
BranchCache configuration 339
for setting up CIFS server 37
Previous Versions
considerations when restoring folders with junctions 318
creating a Snapshot configuration to enable access 318
determining whether Snapshot copies are available for use 316
recover files and folders with, Microsoft 315
requirements for using 315
Previous Versions tab
using to view and manage Snapshot copy data 316
priorities
how FPolicy manages processing FPolicy policy 456
privileged data access
what it means to grant super user credentials for FPolicy 456
privileges
adding to local or domain users or groups 234
defined, local 216
displaying overrides 237
how to assign local 217
list of supported local 216
predefined BUILTIN group default 218
removing from local or domain users or groups 235
resetting for local or domain users or groups 236
SeChangeNotifyPrivilege, adding to enable bypass
traverse checking 239
SeChangeNotifyPrivilege, disallowing users and
groups from bypass traverse checking by removing 240
SeChangeNotifyPrivilege, information about
configuring for bypass traverse checking 237
processes
how Data ONTAP auditing works 422
profiles
advantages of storing user profiles on roaming 311
configuring roaming 312
requirements for using roaming 311
protocols
file locking between, explained 294
how Witness works 377
modifying for SVMs 136
support requirements for BranchCache 337
that FPolicy can monitor 453
that provide nondisruptive operation capabilities for
Hyper-V and SQL Server over SMB 374
public access
enabling or disabling to user home directories 329
Q
qtrees
commands for enabling or disabling oplocks on 110
configuring security style on 147
configuring Storage-Level Access Guard on 154
displaying file security information for Storage-
Level Access Guard security 158
removing Storage-Level Access Guard 160
when you can enable or disable oplocks on 110

R
read-only bits
how Data ONTAP treats 294
recommendations
BranchCache configuration 339
for Hyper-V over SMB configurations 389
for SQL Server over SMB configurations 389
FPolicy setup 462
SMB signing configuration 87
recover files and folders
Previous Versions 315
redirection
introduction to storing data on a CIFS server using folder 312
requirements for using folder 313
rediscovering
Active Directory LDAP servers and domain controllers 33
LDAP servers and domain controllers 130
trusted domains used for multidomain name mapping searches 169
referrals
considerations and requirements when using SMB automatic node 365
support for SMB automatic node 367
relative symbolic links
creating for SMB shares 335
how SMB clients can access UNIX 331
remote offices
where to find information about configuring BranchCache at 343
Remote VSS
backups, how SnapManager for Hyper-V manages 380
concepts defined 378
considerations when using with Hyper-V over SMB configurations 388
defined 378
example of directory structure used by 379
process when using SnapManager for Hyper-V 380
use for share-based backups of Hyper-V virtual machines 378
removing
NetBIOS aliases for CIFS servers, command for 140
preferred domain controllers for Active Directory computer accounts 34
preferred domain controllers, command for 132
preferred trusted domains used for multidomain name mapping searches 170
privileges from local or domain groups 235
share properties on existing SMB shares 183
shares properties from existing SMB shares, command for 186
Storage-Level Access Guard 160
users from local groups 230
renaming
local groups 228
local user accounts 223
replacing
preferred trusted domains used for multidomain name mapping searches 170
required password complexity
enabling or disabling for local users 80
required SMB signing
enabling or disabling 88
requirements
auditing configuration 424
BranchCache network protocol support 337
CIFS server, for Hyper-V over SMB configurations 384
CIFS server, for SQL Server over SMB configurations 385
Data ONTAP and licensing, for Hyper-V over SMB configurations 383
Data ONTAP and licensing, for SQL Server over SMB configurations 383
Data ONTAP version requirements for BranchCache 337
for FPolicy scope configurations if using the FPolicy policy uses the native engine 481
for IPv6 with SMB 141
for SMB automatic node referrals 365
for using folder redirection 313
for using GPOs with CIFS servers 118
for using ODX 361
for using offline files 308
FPolicy setup 461
Hyper-V over SMB configuration 386
network and data LIF, for Hyper-V over SMB configurations 383
network and data LIF, for SQL Server over SMB configurations 383
Previous Versions use 315
SQL Server over SMB configuration 387
volume, for Hyper-V over SMB configurations 384
volume, for SQL Server over SMB configurations 385
when using BUILTIN groups 217
Windows host version requirements for BranchCache 337
resetting
Active Directory LDAP servers and domain controllers 33
LDAP servers and domain controllers 130
passwords for Active Directory computer accounts on SVMs 31
passwords for CIFS servers machine accounts, command for 140
privileges for local or domain groups 236
privileges for local or domain users 236
resetting and rediscovering
servers for CIFS servers, command for 140
Resource
KDC, support for SID Compression 22
restore
considerations when restoring folders with junctions with Previous Versions 318
restrict anonymous option
configuring CIFS access restrictions for anonymous users 74
restrictions
when choosing authentication methods for cluster-scoped FPolicy external engines with MetroCluster and SVM disaster recovery.

revert considerations
for Hyper-V over SMB configurations when local users and groups are configured.
reverting considerations for FPolicy passthrough-read functionality.
considerations for SQL Server over SMB configured for nondisruptive operations.
process when there are audit-enabled SVMs.
what happens to BranchCache.
roaming profiles
advantages of using to store user profiles.
configuring requirements for using.

root CA certificates
converting copy to ASCII text, self-signed.
exporting copy of self-signed.
installing on the SVM.

root volumes
configuring security style on SVM.
Hyper-V over SMB configurations, verifying NTFS security style.
SQL Server over SMB configurations, verifying NTFS security style.

rotating
audit event logs, manually.
rules
export policy, examples for SMB access.

S
SACLs
adding ACEs to security descriptors.
commands for managing ACEs in NTFS.
defined.
scopes
command for displaying information about FPolicy.
command for modifying FPolicy.
configuration information to gather for FPolicy.
creating FPolicy.
planning the configuration for FPolicy.

search paths
commands for managing.
for home directories, adding.
SeChangeNotifyPrivilege
information about configuring for bypass traverse checking.
privileges, adding to enable bypass traverse checking.
SeChangeNotifyPrivilege privilege
Disallowing users and groups from bypass traverse checking by using.
secure LDAP communications
enabling LDAP over SSL/TLS on the CIFS server for.
security
configuring Storage-Level Access Guard.
Dynamic Access Control, displaying information about.
how security traces work.
how to use Storage-Level Access Guard to secure access to files and folders.
limits for using the CLI to set file and folder.
removing Storage-Level Access Guard.
three levels used to secure file and folder access.
use cases for using Storage-Level Access Guard.
use cases for using the CLI to set file and folder.
verifying applied file and folder.
security certificates
for SSL authentication with FPolicy, do not replicate in SVM non-ID-preserve configurations.
security descriptors
adding DACL ACEs to.
adding SACL ACEs to.
commands for managing NTFS.
creating NTFS.
how used to apply file and folder security.

security levels
setting CIFS server LMCompatibilityLevel.
setting CIFS server minimum authentication.

security policies
adding tasks to.
applying to SVMs with FlexVol volumes.
commands for managing.
creating.
monitoring jobs.

security policy jobs
commands for managing.
considerations when managing.

security policy tasks
commands for managing.

security settings
determining whether clients are connected using encrypted SMB sessions.
determining whether SMB sessions are connecting with desired.
displaying information about CIFS server.
introduction to managing on CIFS servers.
modifying CIFS server Kerberos.
on CIFS servers in SVM disaster recovery configurations, important considerations about.
security style
volume or qtree containing the share.
security styles
configuring on FlexVol volumes.
configuring on qtrees.
configuring on SVM root volumes.
data, managing presentation of file security to SMB clients for UNIX.
displaying file security information for NTFS.
security-style volumes.
displaying file security information for UNIX.
security-style volumes.
effects on file permissions.
how inheritance works.
how to choose.
introduction to how they affect data access.
UNIX, how UNIX file permissions provide access control over SMB 196
when and where to set 21
Security tab
how to manage UNIX permissions using Windows 77
security trace filters
creating 286
deleting 290
displaying 287
modifying 289
security trace records
deleting 291
deleting all 292
security trace results
displaying 288
security traces
considerations when creating 284
how it works 283
introduction to performing 285
introduction to verifying or troubleshooting file and directory access with 283
results, how to interpret 292
types of access checks monitored 284
self-signed root CA certificates
converting to ASCII text, copy of 98
exporting copy of 98
installing on the SVM 98
server configuration, CIFS
planning overview 38
server keys
changing BranchCache 348
specifying for BranchCache configurations 340
server setup
decisions to make prior to CIFS 50
servers
commands for managing CIFS 140
displaying information about discovered LDAP and domain controller 130
displaying list of NetBIOS aliases on CIFS 134
enabling LDAP over SSL/TLS on CIFS 97
prerequisites for setting up CIFS 37
resetting and rediscovering LDAP and domain controller 130
supported and unsupported Dynamic Access Control functionality on CIFS 198
servers, CIFS
introduction to configuring 36
list of options 70
SeSecurityPrivilege privilege
adding to the user account used to install SQL Server 402
sessions
displaying information about SMB 298, 415
displaying information about what type of users are connected over SMB 102
setting up
CIFS servers, introduction to 36
LDAP over SSL/TLS, tasks to 97
setup
decisions to make prior to CIFS server 50
prerequisites for CIFS server 37
SFO partner
how it plays the role of witness for transparent failover 377
shadow copies
configuring directory depth of VSS 402
defined 378
shadow copy sets defined 378
share names
static home directory, what happens after upgrading 322
share parameters
using to customize SMB shares when creating 177
share path components
differences between Data ONTAP and Windows handling of locks on 295
share paths
elimination of execute permission on 175
share permissions
configuring SMB 188
default when creating SMB shares 172
share properties
adding or removing on existing SMB shares 183
BranchCache 344
commands for managing SMB 186
using to customize SMB shares when creating 177
share settings
using to customize SMB shares when creating 177
share-based backups
use remote VSS to backup virtual machines 378
share-level ACLs
introduction to managing SMB 187
share-level security
how used to secure access 24
shares
adding home directory 320
configuring existing, for continuous availability 403
configuring offline files support on 310
configuring offline files support on SMB 309
continuously available, creating for Hyper-V and SQL Server over SMB configurations 401
continuously available, verifying configuration of Hyper-V and SQL Server 412
creating NTFS data volumes for continuously available 400
disabling BranchCache on single SMB 355
enabling or disabling access-based enumeration on SMB 371
enabling or disabling oplocks on existing SMB 109
enabling or disabling oplocks when creating SMB 108
information to gather when creating for Hyper-V and SQL Server over SMB configurations 391
introduction to enabling BranchCache on SMB 343
introduction to providing folder security on, with access-based enumeration 370
introduction to securing with access-based enumeration 370
overview of disabling BranchCache on SMB 354
requirements for Hyper-V over SMB 386
requirements for SQL Server over SMB 387
stopping automatic BranchCache caching on all SMB 356
unique user names required for home directories 322
what happens to static home directory share names after upgrading 322
See also SMB shares
shares, SMB
information needed when creating 176
show commands
how they work when displaying FPolicy configuration 492
SID compression
support for KDC Resource 22
signing
monitoring statistics for SMB 90
SLAG
See Storage-Level Access Guard
SMB
about using BranchCache for caching at branch offices 336
adding SeSecurityPrivilege privilege to the user account used to install SQL Server 402
commands for managing access control lists 190
commands for managing NFS character mapping to 163
configuring lifetime of metadata cache entries 293
considerations and requirements when using SMB automatic node referrals 365
creating NTFS data volumes for continuously available shares 400
differences between Data ONTAP and Windows handling of locks on share path components 295
displaying IPv6 session information 144
displaying statistics 305, 409
enabling IPv6 on the cluster for 144
enabling or disabling 2.x on SVMs with FlexVol volumes 106
enabling or disabling automatic node referrals on CIFS servers 368
enabling or disabling required password complexity for local users 80
enabling the metadata cache 293
events that can be audited 426
file and directory naming dependencies 145
file locking between protocols explained 294
how automatic node referrals improve client response time 364
how Data ONTAP treats read-only bits 294
how Data ONTAP uses share-level ACLs 188
how metadata caching works for 293
how name mapping is used for access 23
how signing policies affect communications 85
how to disable IPv6 on the cluster 144
how to use SMB encryption to enhance security for data transfers over 92
introduction to managing share-level ACLs 187
IPv6 network supported for SMB access 141
IPv6 requirements 141
IPv6 support with 142
Kerberos authentication 22
modifying protocols for SVMs 136
monitoring SMB signing statistics 90
NTLM authentication 23
requirements for using folder redirection 313
requirements for using offline files 308
requirements for using roaming profiles 311
signing, performance impact of 87
statistics, determining which counters and objects are available 303, 407
support for automatic node referrals 367
supported 1.0 functionality 103
supported 2.0 durable handle functionality 103
supported 2.0 functionality 103
supported clients 37
supported domain controllers 37
unsupported 2.0 functionality 103
unsupported 2.1 functionality 104
using statistics counters to monitor automatic node referral activity 368
versions supported on SVMs with FlexVol volumes 103
versions supported on SVMs with Infinite Volumes 103
versions that support Previous Versions 315
where to find information about support, on Infinite Volumes 69
SMB 3.0
creating continuously available shares for Hyper-V and SQL server over SMB configurations 401
displaying continuously available protection information 298, 415
enabling or disabling on SVMs with FlexVol volumes 107
how functionality supports nondisruptive operations for Hyper-V and SQL Server over SMB 376
requirements for using ODX 361
supported functionality 105
supported nondisruptive operations 105
unsupported functionality 105
SMB access
configuring UNIX symbolic link support for 334
considerations when reverting export policies for 211
creating symbolic link mappings for 335
enabling or disabling export policies for 207
enabling or disabling local user authentication for 220
enabling or disabling local users and groups for 219
examples of export policy rules to allow 209
how export polices are used for 205
how export policies are handled after Data ONTAP upgrade 206
how to use UNIX symbolic links for 331
limits when configuring UNIX symbolic links for 332
role authentication plays for 22
role that export policies play with 24
when UNIX file permissions are used to provide access control for 196
SMB clients
advantages of using NTFS ACLs for presentation of UNIX security-style data to 75
configuring character mapping for file name translation on FlexVol volumes 161
enabling or disabling presentation of NTFS ACLs for UNIX security-style data 76
managing presentation of file security to, for UNIX data 75
using oplocks to improve performance on 107
SMB encryption
determining whether clients are using with SMB
sessions 94
how to use to enhance security for data transfers over
SMB 92
required, enabling or disabling on the CIFS server
for incoming SMB traffic 93
SMB file access
introduction to setting up 145
understanding with Data ONTAP 15
SMB home directories
adding search paths 322
creating configurations using %u 325
creating configurations using %w and %d 323
how clustered Data ONTAP enables dynamic 319
introduction to managing 319
SMB home directory shares
adding 320
SMB open files
displaying information about 298, 301, 418
SMB security traces
considerations when creating 284
creating filters 286
deleting all records 292
deleting filters 290
deleting records 291
displaying filters 287
displaying results 288
how it works 283
how to interpret results 292
introduction to performing 285
modifying filters 289
types of access checks monitored for 284
SMB sessions
determining whether clients are connected using
encrypted 94
determining whether they are signed 89
displaying information about 298, 415
displaying information about what type of users are
connected over 102
displaying IPv6 information about 144
SMB shares
adding home directory 320
adding or removing share properties on existing 183
adding search paths for home directories 322
BranchCache configuration recommendations 339
commands for managing 186
configuring existing shares for continuous
availability 403
configuring folder redirection 313
configuring offline files support on 309
configuring permissions on 188
configuring UNIX symbolic link support on 334
configuring VSS shadow directory depth 402
connecting the SVM to the MMC to view 186
continuously available, verifying configuration of
Hyper-V and SQL Server 412
creating access control lists for 188
creating home directories configurations using %u
325
creating home directories configurations using %w
and %d 323
creating on CIFS servers 177
creating symbolic link mappings 335
creating with the force-group setting 182
default ACL when creating 172
defined 172
determining Snapshot copy availability for Previous
Versions use 316
disabling BranchCache on single SMB 355
elimination of execute permission on share paths 175
enabling BranchCache on existing 344
enabling BranchCache when creating 343
enabling or disabling access-based enumeration on
371
enabling or disabling oplocks on existing 109
enabling or disabling oplocks when creating 108
force-group setting, what it does 182
how clustered Data ONTAP enables dynamic home
directories on 319
how volume junctions are used with 16
implications of case-sensitivity of directory names
when creating or accessing files in 175
implications of case-sensitivity of file and directory
names when creating or accessing files in a
multiprotocol environment 145
information needed when creating 176
information to gather when creating for Hyper-V and
SQL Server over SMB configurations 391
introduction to configuring metadata caches for 1.0
293
introduction to creating Data ONTAP configurations
for nondisruptive operations with Hyper-V or SQL
Server over 393
introduction to using folder redirection to store data
on a CIFS server 312
managing file access with 212
naming considerations 174
overview of disabling BranchCache on 354
stopping automatic BranchCache caching on all 356
using the Previous Versions tab to view and manage
Snapshot copy data 316
what happens if CIFS servers or SVMs are deleted
172
what the default administrative shares are 173
SMB signing
about using to enhance network security 85
considerations when there are multiple data LIFs 87
Data ONTAP support for 85
enabling or disabling required 88
performance impact of 87
recommendations for configuring 87
SMB statistics
displaying information about 298
SMB users
displaying home directory path information for 329
enabling or disabling required password complexity
for local 80
introduction to configuring default UNIX user
mappings for 99
SnapManager for Hyper-V
how to use to manage Remote VSS-based backups
for Hyper-V over SMB 380
where to find information about configuring 373
SnapManager for Microsoft SQL Server
where to find information about configuring 373
SnapMirror
considerations when using on SVMs with local groups 215
Snapshot copies
configuring to enable Previous Versions access 318
determining availability for Previous Versions use 316
using the Previous Versions tab to view and manage data in 316
space issues
how to troubleshoot staging volume 452
SQL Server
over SMB solutions, how SMB 3.0 functionality supports 376
verifying that automatic node referrals are disabled 399
where to find information about configuring 373
SQL Server over SMB
adding the SeSecurityPrivilege privilege to the user account used to install 402
CIFS server requirements when configuring 385
concepts 374
configurations, creating continuously available shares for 401
configurations, information to gather for creating volumes 390
configured for nondisruptive operations, considerations when reverting 407
configuring existing shares for continuous availability 403
creating NTFS data volumes for continuously available shares 400
Data ONTAP and licensing requirements when configuring 383
how ODX copy offload is used with 381
how to use system health monitor to determine nondisruptive operation status 410
information about configuration requirements and considerations 382
information about managing configurations 403
information about using statistics to monitor SMB activity 407
information to gather for creating continuously available SMB shares 391
introduction to configuration planning tasks 390
introduction to creating Data ONTAP configurations for nondisruptive operations with 393
network and data LIF requirements when configuring 383
nondisruptive operations for, defined 373
protocols that provide capabilities for nondisruptive operations 374
recommendations when configuring for nondisruptive operations 389
requirements and considerations when configuring 387
requirements when using ODX copy offload 389
solutions, how SMB 3.0 functionality supports 376
support for stand-alone and clustered configurations 373
supported nondisruptive operations 373

verifying CIIFS server option settings for NDOs with 398
verifying continuously available SMB share configuration 412
verifying LIF status 413
verifying that domain accounts map to the default UNIX user 395
verifying that root volume is set to NTFS security style 397
volume requirements when configuring 385
what you need to configure 373
SQL Servers
adding SeSecurityPrivilege privilege to the installer's user account 402
SSL
security certificates for FPolicy do not replicate in SVM non-ID-preserve configurations 469
SSL certificates
additional information about configuring for FPolicy external engine connections 469
SSL security
restrictions when choosing authentication methods for cluster-scoped FPolicy external engines with MetroCluster and SVM disaster recovery 470
staging files
defined for auditing 421
how to troubleshoot space issues related to volumes that contain 452
staging volumes
aggregate space considerations when enabling auditing for 424
defined for auditing 421
how to troubleshoot space issues related to 452
starting
CIFS servers 136
CIFS servers, command for 140
statistics
determining which counters and objects are available 303, 407
displaying auditing 305
displaying BranchCache 351
displaying BranchCache hash 305
displaying SMB 409
displaying SMB and CIIFS 305
monitoring SMB signing 90
using counters to monitor SMB automatic node referral activity 368
stopping
CIFS servers 136
CIFS servers, command for 140
Storage-Level Access Guard
adding DACL ACEs for 259
adding SAACL ACEs for 271
adding tasks to security policies for 262, 275
configuration workflow 153
configuring 154
creating security descriptors for 257, 269
displaying information about auditing settings on mixed or NTFS security-style volumes for 248, 445
displaying information about auditing settings on mixed security-style volumes for 250
displaying information about file security settings on mixed security-style volumes for 244
creating broadcast domains for the IP spaces for the CIFS server 56, 57
creating for CIFS server 59
creating FPolicy policies on 487
creating IPspaces for the CIFS server 52
creating LIFs for CIFS servers 61
deleting Active Directory computer accounts for 30
deleting an auditing configuration 450
displaying information about Active Directory computer accounts for) 30
displaying information about discovered Active Directory LDAP servers and domain controllers 32
displaying information about preferred domain controllers for Active Directory computer accounts 35
enabling and disabling auditing on 447
enabling auditing on 438
examples of export policy rules for SMB access 209
for the CIFS server, information to gather before creating 42
how FPolicy manages processing policies 456
how FPolicy services work across namespaces 458
how to choose whether to create an Active Directory computer account or a CIFS server 26, 36
how to troubleshoot space issues related to staging volumes on 452
important considerations about CIFS server security settings in disaster recovery configurations for 79
information to gather before creating CIFS servers on 49
information to gather for creating data LIFs on 44
installing root CA self-signed certificate for LDAP over SSL/TLS on 98
introduction to auditing NAS file access events 421
introduction to managing NTFS file security and audit policies using the CLI 251
joining to Active Directory domain 139
major steps in setting up the CIFS server 50
modifying protocols 136
moving CIFS servers to different OUs 137
requirements for using ODX for copy offloads 361
resetting and rediscovering Active Directory LDAP servers and domain controllers on 33
revert process when there are audit-enabled 451
role with FPolicy implementations 454
security certificates do not replicate in a non-ID-preserve disaster recovery relationship 469
stopping or starting CIFS servers on 136
supported GPOs on CIFS servers 113
supported SMB 1.0 functionality 103
supported SMB 2.0 functionality 103
supported SMB 2.1 functionality 104
supported SMB 3.0 functionality 105
using FPolicy for file monitoring and management 453
viewing SMB shares by using the MMC to connect to 186
what happens to SMB shares when deleting 172
SVMs with FlexVol volumes
applying security policies to 265, 278
symbolic link mappings
commands for managing 336
symbolic links

subnet configuration
information to gather before creating CIFS servers 39
suggestions
how to send feedback about documentation 501
super user credentials
what it means to grant for FPolicy privileged data access 456
support
for IPv6 with SMB and CIFS services 142
supported
GPOs 113
local privileges 216
supported versions
configuring BranchCache 340
SMB on SVMs with FlexVol volumes 103
SMB on SVMs with Infinite Volumes 103
SVM configurations
restrictions when choosing authentication methods for cluster-scoped FPolicy external engines with 470
SVM disaster recovery
important considerations about CIFS server security settings in configurations for 79
SVM disaster recovery configurations
restrictions when choosing authentication methods for cluster-scoped FPolicy external engines with 470
SVMs
(configuring and managing Active Directory computer accounts (no CIFS license) 26
actions you must take before revert when there are audit-enabled 451
adding CIFS server preferred domain controllers 131
adding or removing preferred domain controllers for Active Directory computer accounts 34
applying GPOs to CIFS servers 113
commands for modifying auditing configurations 449
configuring dynamic DNS before moving the CIFS server to another domain 138
configuring security style on root volume 147
considerations when choosing BranchCache hash store location 338
considerations when configuring multiple data LIFs 87
creating a file and directory auditing configuration on 436
creating Active Directory computer accounts for (no CIFS license) 27
creating auditing configuration for file and directory events on 436
displaying information about discovered Active Directory LDAP servers and domain controllers 32
displaying information about preferred domain controllers for Active Directory computer accounts 35
displaying security information for volumes or qtrees with 158
displaying security information for volumes or qtrees with 152
how used to secure access 24
introduction to displaying information about 240
introduction to managing file security and audit policies using the CLI for 251
removing 160
use cases for using 153

Index | 527
configuring support for UNIX, on SMB shares 334
creating mappings for SMB shares 335
how SMB clients can access UNIX 331
how to control automatic DFS advertisements that are used with 77, 332
limits when configuring for SMB access 332

symlinks
considerations when auditing 429
See also symbolic links

synchronous
communication, how privileged data access channels are used with 455
FPolicy applications 454
FPolicy notifications, defined 453

system access control lists
See SACLs

system health monitor
how to determine status of nondisruptive operations for Hyper-V and SQL Server over SMB configurations 410

T

tasks
adding to audit and file security policies 262, 275
commands for managing security policy 282

terminology
LDAP over SSL/TLS 95

time services
configuring prior to creating CIFS servers 52
information to gather for setting up on the cluster 38
tokens
ODX 360
trace filters
creating 286
deleting 290
displaying 287
modifying 289

trace records
deleting all 292
deleting security 291
traces
how to interpret results of security 292
introduction to performing security 285
security, displaying results 288
security, how it works 283
types of security access checks monitored 284

traditional oplocks
improving SMB client performance with 107

transparent failover
how Witness protocol enhances 376

traversed directories
disallowing users and groups from bypassing 240

troubleshooting
auditing event log volume space issues 451
staging volume space issues 452
trusted domains
adding, removing, or replacing trusted domains from the list of preferred 170
discovered, how used with multidomain searches for user name mapping 166
displaying information about discovered 170
displaying information about the list of preferred 171
rediscovering, used for multidomain name mapping searches 169
twitter
how to receive automatic notification of documentation changes 501

U

understanding
SMB file access with Data ONTAP 15
UNIX
displaying file security information on UNIX
security-style volumes 246
file security on mixed volumes, displaying information about 244
security-style data, enabling or disabling presentation of NTFS ACLs to SMB clients for 76
security-style data, managing presentation of file security to SMB clients for 75
UNIX identities
introduction to mapping Windows identities to 163
UNIX permissions
how Data ONTAP preserves 77
how to manage using Windows Security tab 77
when used to provide access control over SMB 196
UNIX symbolic links
configuring support for, on SMB shares 334
creating mappings for SMB shares 335
introduction to configuring SMB client access to 330
limits when configuring for SMB access 332
UNIX users
configuring default 99
UNIX users and groups
introduction to using to configure SMB share-level ACLs 187

unmounting
volumes in NAS namespaces 150

unsupported features
Windows 37
updates
how performed for GPOs on a CIFS server 119
what to do for failing GPO 119

upgrading
considerations for FPolicy passthrough-read functionality 462
what happens to static home directory share names after 322

use cases
for ODX 363
for using Storage-Level Access Guard 153
for using the CLI to set file and folder security 252
user access tokens
how they are constructed 214
user accounts
changing passwords 224
configuring guest UNIX account 100
Creating local 221
deleting local 226
displaying information about local 225
enabling or disabling local 224
local, displaying information about local group membership 225
modifying, renaming, enabling, or disabling local 223
user home directories
enabling or disabling access to 329
user mappings
introduction to configuring default 99
user name mappings
preferred trusted domains used with multidomain search for 166
user names
how mapping works 23
must be unique for home directory shares 322
user types
connected over SMB sessions, displaying information about 102
users
adding privileges to local or domain 234
changing local account passwords 224
configuring default UNIX 99
creating local accounts 221
deleting CIFS servers, what happens to local 215
deleting local accounts 226
disallowing from bypassing directory traverse checking 240
displaying information about local 225
enabling or disabling local accounts 224
how access tokens are constructed for local 214
local, displaying information about local group membership 225
local, how authentication works 214
modifying, renaming, enabling, or disabling local accounts 223
password requirements for local 217
removing privileges from local or domain 235
resetting privileges for local or domain 236
revert considerations when there are local 215
updating names in the local databases for domain 232
users and groups
how Data ONTAP uses local 212
local, defined 212
local, using for authentication and authorization 212
users and groups)
Windows and UNIX, introduction to using to configure SMB share-level ACLs 187
using
options to customize CIFS servers 70
Previous Versions tab to view and manage Snapshot copy data 316

V

Verifying
applied audit policies 279
applied file and folder security 266
auditing configuration 438, 448
automatic node referrals are disabled for Hyper-V over SMB configurations 399
automatic node referrals are disabled for SQL Server over SMB configurations 399
CIFS server option settings for Hyper-V over SMB configurations 398
CIFS server option settings for NDVs with SQL Server over SMB configurations 398
continuously available configuration of shares for Hyper-V and SQL Server SMB configurations 412
Hyper-V and SQL Server domain accounts map to the default UNIX user 395
Kerberos and NTLMv2 authentication are permitted with Hyper-V over SMB configuration 394
LIF status for Hyper-V and SQL Server over SMB configurations 413
NTFS security style on root volume for Hyper-V over SMB configurations 397
NTFS security style on root volume for SQL Server over SMB configurations 397
version support
modifying for BranchCache configurations 346
versions
supported BranchCache 337
viewing
audit event logs 425
local users and groups from the Microsoft Management Console 215
volume junctions
defined 15
how they affect SMB access 15
how used in SMB and NFS namespaces 16
usage rules 15
volume roots
elimination of execute permission requirement for SMB shares when accessing 175
volume size for hash store
increasing for BranchCache configurations 346
volumes
aggregate space considerations when enabling auditing for staging 424
commands for enabling or disabling oplocks on 110
commands for managing NFS to SMB character mapping on FlexVol 163
configuring character mappings for SMB file name translation on FlexVol 161
configuring security style on FlexVol 147
configuring Storage-Level Access Guard on 154
creating with specified junction points 148
creating without specified junction points 149
displaying Dynamic Access Control security information on NTFS and mixed security-style 203
displaying file security information for NTFS security-style 242
displaying file security information for Storage-Level Access Guard security 158
displaying file security information on mixed security-style 244
displaying file security information on UNIX security-style 246
displaying information about Storage-Level Access Guard auditing settings for NTFS or mixed security-style 248, 445
displaying information about Storage-Level Access Guard auditing settings on mixed security-style 250
displaying information about Storage-Level Access Guard file security settings for mixed security-style 244
displaying information about Storage-Level Access Guard file security settings for NTFS security-style 242
displaying mount and junction point information 151
elimination of execute permission requirement for SMB shares when accessing root of 175
how junction points are used to create namespaces with 15
how to troubleshoot space issues related to staging 452
how to use Storage-Level Access Guard to secure access to files and folders on 152
information to gather when creating for Hyper-V and SQL Server over SMB configurations 390
introduction to creating and managing in NAS namespaces 148
introduction to displaying information about file security on 240
introduction to displaying information about Storage-Level Access Guard security on FlexVol 240
introduction to displaying information audit policy on FlexVol 240
mounting and unmounting in NAS namespaces 150
NTFS, creating for continuously available shares 400
removing Storage-Level Access Guard requirements for Hyper-V over SMB 160
requirements for SQL Server over SMB 385
when you can enable or disable oplocks on 110
where to find information about SMB support on Infinite 69
Vservers
See SVMs
VSS shadow copies
configuring directory depth 402
enabling or disabling 405
introduction to configuring SMB client access using Windows 330
enabling or disabling guest UNIX user account 100
unsupported features 37
Windows administrator access enabling or disabling to user home directories 329
Windows administrators group mapping to root 101
Windows clients how SMB signing policies affect SMB communication 85
where to get information about configuring BranchCache on 343
Windows groups deleting local 231
Windows identities introduction to mapping to UNIX identities 163
Windows Security tab how to manage UNIX permissions using 77
Windows user accounts creating local 221
Windows users and groups introduction to using to configure SMB share-level ACLs 187
Witness protocol how it enhances transparent failover 376
how it works 377
workflows Storage-Level Access Guard configuration 153
worksheets for recording information needed to configure FPolicy events 477
for recording information needed to configure FPolicy external engines 470
for recording information needed to configure FPolicy policies 482
for recording information needed to configure FPolicy scopes 484
write cache data loss considerations when using oplocks 108
W
widelinks how SMB clients can access UNIX symbolic links 331
XML file format, viewing audit event logs with 425
supported audit event log file format 425
X