## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deciding whether to use this guide</td>
<td>4</td>
</tr>
<tr>
<td>Administrator authentication and RBAC workflow</td>
<td>5</td>
</tr>
<tr>
<td>Worksheets for administrator authentication and RBAC configuration</td>
<td>6</td>
</tr>
<tr>
<td>Creating login accounts</td>
<td>14</td>
</tr>
<tr>
<td>Enabling local account access</td>
<td>14</td>
</tr>
<tr>
<td>Enabling password account access</td>
<td>15</td>
</tr>
<tr>
<td>Enabling SSH public key accounts</td>
<td>15</td>
</tr>
<tr>
<td>Enabling SSH multifactor authentication (MFA)</td>
<td>16</td>
</tr>
<tr>
<td>Enabling SSL certificate accounts</td>
<td>17</td>
</tr>
<tr>
<td>Enabling Active Directory account access</td>
<td>18</td>
</tr>
<tr>
<td>Enabling LDAP or NIS account access</td>
<td>19</td>
</tr>
<tr>
<td>Configuring SAML authentication</td>
<td>20</td>
</tr>
<tr>
<td>Managing access-control roles</td>
<td>22</td>
</tr>
<tr>
<td>Modifying the role assigned to an administrator</td>
<td>22</td>
</tr>
<tr>
<td>Defining custom roles</td>
<td>23</td>
</tr>
<tr>
<td>Predefined roles for cluster administrators</td>
<td>24</td>
</tr>
<tr>
<td>Predefined roles for SVM administrators</td>
<td>24</td>
</tr>
<tr>
<td>Managing administrator accounts</td>
<td>27</td>
</tr>
<tr>
<td>Associating a public key with an administrator account</td>
<td>27</td>
</tr>
<tr>
<td>Generating and installing a CA-signed server certificate</td>
<td>28</td>
</tr>
<tr>
<td>Generating a certificate signing request</td>
<td>28</td>
</tr>
<tr>
<td>Installing a CA-signed server certificate</td>
<td>29</td>
</tr>
<tr>
<td>Configuring Active Directory domain controller access</td>
<td>30</td>
</tr>
<tr>
<td>Configuring an authentication tunnel</td>
<td>30</td>
</tr>
<tr>
<td>Creating an SVM computer account on the domain</td>
<td>31</td>
</tr>
<tr>
<td>Configuring LDAP or NIS server access</td>
<td>32</td>
</tr>
<tr>
<td>Configuring LDAP server access</td>
<td>32</td>
</tr>
<tr>
<td>Configuring NIS server access</td>
<td>33</td>
</tr>
<tr>
<td>Creating a name service switch</td>
<td>34</td>
</tr>
<tr>
<td>Changing an administrator password</td>
<td>34</td>
</tr>
<tr>
<td>Locking and unlocking an administrator account</td>
<td>35</td>
</tr>
<tr>
<td>Managing failed login attempts</td>
<td>36</td>
</tr>
<tr>
<td>Enforcing SHA-2 on administrator account passwords</td>
<td>36</td>
</tr>
<tr>
<td>Where to find additional information</td>
<td>38</td>
</tr>
<tr>
<td>Copyright information</td>
<td>39</td>
</tr>
<tr>
<td>Trademark information</td>
<td>40</td>
</tr>
<tr>
<td>How to send comments about documentation and receive update notifications</td>
<td>41</td>
</tr>
<tr>
<td>Index</td>
<td>42</td>
</tr>
</tbody>
</table>
Deciding whether to use the Administrator Authentication and RBAC Power Guide

This guide describes how to enable login accounts for ONTAP cluster administrators and storage virtual machine (SVM) administrators, and how to use role-based access control (RBAC) to define the capabilities of administrators.

You should use this guide if you want to enable login accounts and RBAC in the following way:

- You want to use the ONTAP command-line interface (CLI), not OnCommand System Manager or an automated scripting tool.
- You want to use best practices, not explore every available option.
- You do not want to read a lot of conceptual background.
- You are not using SNMP to collect information about the cluster.

If this guide is not suitable for your situation, you should see the following documentation instead:

- ONTAP 9 commands
- Cluster management using System Manager
- NetApp Documentation: OnCommand Workflow Automation (current releases)
Administrator authentication and RBAC workflow

You can enable authentication for local administrator accounts or remote administrator accounts. The account information for a local account resides on the storage system and the account information for a remote account resides elsewhere. Each account can have a predefined role or a custom role.

You can enable local administrator accounts to access an admin storage virtual machine (SVM) or a data SVM with the following types of authentication:

- Password
- SSH public key
- SSL certificate
- SSH multifactor authentication (MFA)
  Starting with ONTAP 9.3, authentication with password and public key is supported.

You can enable remote administrator accounts to access an admin SVM or a data SVM with the following types of authentication:

- Active Directory
- SAML authentication (only for admin SVM)
  Starting with ONTAP 9.3, Security Assertion Markup Language (SAML) authentication can be used for accessing the admin SVM by using any of the following web services: Service Processor Infrastructure, ONTAP APIs, or OnCommand System Manager.
  Starting with ONTAP 9.4, SSH MFA can be used for remote users on LDAP or NIS servers. Authentication with nsswitch and public key is supported.
Worksheets for administrator authentication and RBAC configuration

Before creating login accounts and setting up role-based access control (RBAC), you should gather information for each item in the configuration worksheets.

Creating or modifying login accounts

You provide these values with the `security login create` command when you enable login accounts to access a storage virtual machine (SVM). You provide the same values with the `security login modify` command when you modify how an account accesses an SVM.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-vserver</code></td>
<td>The name of the SVM that the account accesses. The default value is the name of the admin SVM for the cluster.</td>
<td></td>
</tr>
<tr>
<td><code>-user-or-group-name</code></td>
<td>The user name or group name of the account. Specifying a group name enables access to each user in the group. You can associate a user name or group name with multiple applications.</td>
<td></td>
</tr>
<tr>
<td><code>-application</code></td>
<td>The application that is used to access the SVM:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>http</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>ontapi</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>snmp</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>ssh</code></td>
<td></td>
</tr>
<tr>
<td><code>-authmethod</code></td>
<td>The method that is used to authenticate the account:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>cert</code> for SSL certificate authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>domain</code> for Active Directory authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>nsswitch</code> for LDAP or NIS authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>password</code> for user password authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>publickey</code> for public key authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>community</code> for SNMP community strings</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>usm</code> for SNMP user security model</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>saml</code> for Security Assertion Markup Language (SAML) authentication</td>
<td></td>
</tr>
<tr>
<td><code>-remote-switch-ipaddress</code></td>
<td>The IP address of the remote switch. The remote switch can be a cluster switch monitored by the cluster switch health monitor (CSHM) or a Fibre Channel (FC) switch monitored by the MetroCluster health monitor (MCC-HM). This option is applicable only when the application is <code>snmp</code> and the authentication method is <code>usm</code>.</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Your value</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>-role</td>
<td>The access control role that is assigned to the account:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• For the cluster (the admin SVM), the default value is <strong>admin</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• For a data SVM, the default value is <strong>vsadmin</strong>.</td>
<td></td>
</tr>
<tr>
<td>-comment</td>
<td>Optional. Descriptive text for the account. You should enclose the text in</td>
<td></td>
</tr>
<tr>
<td></td>
<td>double quotation marks (&quot;&quot;&quot;).</td>
<td></td>
</tr>
<tr>
<td>-is-ns-switch-group</td>
<td>Whether the account is an LDAP group account or NIS group account (yes or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>no).</td>
<td></td>
</tr>
<tr>
<td>-second-authentication-</td>
<td>Second authentication method in case of multifactor authentication in ONTAP</td>
<td></td>
</tr>
<tr>
<td>method</td>
<td>9.3:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>none</strong> if not using multifactor authentication, default value</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>publickey</strong> for public key authentication when the authmethod is password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>or nsswitch</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>password</strong> for user password authentication when the authmethod is public</td>
<td></td>
</tr>
<tr>
<td></td>
<td>key</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>nsswitch</strong> for user password authentication when the authmethod is public</td>
<td></td>
</tr>
<tr>
<td></td>
<td>key</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Support for nsswitch is available from ONTAP 9.4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The order of authentication is always public key followed by password.</td>
<td></td>
</tr>
</tbody>
</table>

**Defining custom roles**

You provide these values with the `security login role create` command when you define a custom role.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>-vserver</td>
<td>Optional. The name of the SVM that is associated with the role.</td>
<td></td>
</tr>
<tr>
<td>-role</td>
<td>The name of the role.</td>
<td></td>
</tr>
<tr>
<td>-cmddirname</td>
<td>The command or command directory to which the role gives access. You should</td>
<td></td>
</tr>
<tr>
<td></td>
<td>enclose command subdirectory names in double quotation marks (&quot;&quot;&quot;). For example,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;volume snapshot&quot;.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You must enter <strong>DEFAULT</strong> to specify all command directories.</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Your value</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>-access</td>
<td>Optional. The access level for the role.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For command directories:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>none</strong> (the default value for custom roles) denies access to commands in the command directory</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>readonly</strong> grants access to the <strong>show</strong> commands in the command directory and its subdirectories</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>all</strong> grants access to all of the commands in the command directory and its subdirectories</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For <strong>nonintrinsic commands</strong> (commands that do not end in create, modify, delete, or show):</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>none</strong> (the default value for custom roles) denies access to the command</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>readonly</strong> is not applicable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>all</strong> grants access to the command</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To grant or deny access to intrinsic commands, you must specify the command directory.</td>
<td></td>
</tr>
<tr>
<td>-query</td>
<td>Optional. The query object that is used to filter the access level, which is specified in the form of a valid option for the command or for a command in the command directory. You should enclose the query object in double quotation marks (&quot;&quot;&quot;). For example, if the command directory is volume, the query object &quot;-aggr aggr0&quot; would enable access for the aggr0 aggregate only.</td>
<td></td>
</tr>
</tbody>
</table>

**Associating a public key with a user account**

You provide these values with the `security login publickey create` command when you associate an SSH public key with a user account.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>-vserver</td>
<td>Optional. The name of the SVM that the account accesses.</td>
<td></td>
</tr>
<tr>
<td>-username</td>
<td>The user name of the account.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The default value, <strong>admin</strong>, which is the default name of the cluster administrator.</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Your value</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>-index</td>
<td>The index number of the public key. The default value is 0 if the key is the first key that is created for the account; otherwise, the default value is one more than the highest existing index number for the account.</td>
<td></td>
</tr>
<tr>
<td>-publickey</td>
<td>The OpenSSH public key. You should enclose the key in double quotation marks (&quot;&quot;`).</td>
<td></td>
</tr>
<tr>
<td>-role</td>
<td>The access control role that is assigned to the account.</td>
<td></td>
</tr>
<tr>
<td>-comment</td>
<td>Optional. Descriptive text for the public key. You should enclose the text in double quotation marks (&quot;&quot;`).</td>
<td></td>
</tr>
</tbody>
</table>

### Installing a CA-signed server digital certificate

You provide these values with the `security certificate generate-csr` command when you generate a digital certificate signing request (CSR) for use in authenticating an SVM as an SSL server.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>-common-name</td>
<td>The name of the certificate, which is either a fully qualified domain name (FQDN) or a custom common name.</td>
<td></td>
</tr>
<tr>
<td>-size</td>
<td>The number of bits in the private key. The higher the value, the more secure the key. The default value is 2048. Possible values are 512, 1024, 1536, and 2048.</td>
<td></td>
</tr>
<tr>
<td>-country</td>
<td>The country of the SVM, in a two-letter code. The default value is US. See the man pages for a list of codes.</td>
<td></td>
</tr>
<tr>
<td>-state</td>
<td>The state or province of the SVM.</td>
<td></td>
</tr>
<tr>
<td>-locality</td>
<td>The locality of the SVM.</td>
<td></td>
</tr>
<tr>
<td>-organization</td>
<td>The organization of the SVM.</td>
<td></td>
</tr>
<tr>
<td>-unit</td>
<td>The unit in the organization of the SVM.</td>
<td></td>
</tr>
<tr>
<td>-email-addr</td>
<td>The email address of the contact administrator for the SVM.</td>
<td></td>
</tr>
</tbody>
</table>
### Field: `-hash-function`

The cryptographic hashing function for signing the certificate. The default value is **SHA256**. Possible values are **SHA1**, **SHA256**, and **MD5**.

You provide these values with the `security certificate install` command when you install a CA-signed digital certificate for use in authenticating the cluster or SVM as an SSL server. Only the options that are relevant to this guide are shown in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-hash-function</code></td>
<td>The cryptographic hashing function for signing the certificate. The default value is <strong>SHA256</strong>. Possible values are <strong>SHA1</strong>, <strong>SHA256</strong>, and <strong>MD5</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Active Directory domain controller access

You provide these values with the `security login domain-tunnel create` command when you have already configured a CIFS server for a data SVM and you want to configure the SVM as a gateway or tunnel for Active Directory domain controller access to the cluster.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-vserver</code></td>
<td>The name of the SVM on which the certificate is to be installed.</td>
<td></td>
</tr>
</tbody>
</table>

### Field: `-type`

The certificate type:
- **server** for server certificates and intermediate certificates
- **client-ca** for the public key certificate of the root CA of the SSL client
- **server-ca** for the public key certificate of the root CA of the SSL server of which ONTAP is a client
- **client** for a self-signed or CA-signed digital certificate and private key for ONTAP as an SSL client

You provide these values with the `vserver active-directory create` command when you have not configured a CIFS server and you want to create an SVM computer account on the Active Directory domain.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-vserver</code></td>
<td>The name of the SVM for which the CIFS server has been configured.</td>
<td></td>
</tr>
<tr>
<td><code>-account-name</code></td>
<td>The NetBIOS name of the computer account.</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring LDAP or NIS server access

You provide these values with the `vserver services name-service ldap client create` command when you create an LDAP client configuration for the SVM.

**Note:** Starting with ONTAP 9.2, the `-ldap-servers` field replaces the `-servers` field. This new field can take either a host name or an IP address as the value for the LDAP server.

Only the options that are relevant to this guide are shown in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-domain</code></td>
<td>The fully qualified domain name (FQDN).</td>
<td></td>
</tr>
<tr>
<td><code>-ou</code></td>
<td>The organizational unit in the domain. The default value is <code>CN=Computers</code>. ONTAP appends this value to the domain name to produce the Active Directory distinguished name.</td>
<td></td>
</tr>
</tbody>
</table>

### Worksheets for administrator authentication and RBAC configuration

Worksheets for administrator authentication and RBAC configuration | 11

You provide these values with the `vserver services name-service ldap create` command when you associate an LDAP client configuration with the SVM.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-vserver</code></td>
<td>The name of the SVM with which the client configuration is to be associated.</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Your value</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>-client-config</td>
<td>The name of the client configuration.</td>
<td></td>
</tr>
<tr>
<td>-client-enabled</td>
<td>Whether the SVM can use the LDAP client configuration (true or false).</td>
<td></td>
</tr>
</tbody>
</table>

You provide these values with the `vserver services name-service nis-domain create` command when you create an NIS domain configuration on an SVM.

**Note:** Starting with ONTAP 9.2, the `-nis-servers` field replaces the `-servers` field. This new field can take either a host name or an IP address as the value for the NIS server.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>-vserver</td>
<td>The name of the SVM on which the domain configuration is to be created.</td>
<td></td>
</tr>
<tr>
<td>-domain</td>
<td>The name of the domain.</td>
<td></td>
</tr>
<tr>
<td>-active</td>
<td>Whether the domain is active (true or false).</td>
<td></td>
</tr>
<tr>
<td>-servers</td>
<td>ONTAP 9.0, 9.1: A comma-separated list of IP addresses for the NIS servers that are used by the domain configuration.</td>
<td></td>
</tr>
<tr>
<td>-nis-servers</td>
<td>ONTAP 9.2: A comma-separated list of IP addresses and host names for the NIS servers that are used by the domain configuration.</td>
<td></td>
</tr>
</tbody>
</table>

You provide these values with the `vserver services name-service ns-switch create` command when you specify the look-up order for name service sources.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>-vserver</td>
<td>The name of the SVM on which the name service look-up order is to be configured</td>
<td></td>
</tr>
</tbody>
</table>
| -database | The name service database:  
- **hosts** for files and DNS name services  
- **group** for files, LDAP, and NIS name services  
- **passwd** for files, LDAP, and NIS name services  
- **netgroup** for files, LDAP, and NIS name services  
- **namemap** for files and LDAP name services | |
### Configuring SAML access

Starting with ONTAP 9.3, you provide these values with the `security saml-sp create` command to configure SAML authentication.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-sources</code></td>
<td>The order in which to look up name service sources (in a comma-separated list):</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>files</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>dns</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>ldap</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>nis</code></td>
<td></td>
</tr>
<tr>
<td><code>-idp-uri</code></td>
<td>The FTP address or HTTP address of the Identity Provider (IdP) host from where the IdP metadata can be downloaded.</td>
<td></td>
</tr>
<tr>
<td><code>-sp-host</code></td>
<td>The host name or IP address of the SAML service provider host (ONTAP system). By default, the IP address of the cluster-management LIF is used.</td>
<td></td>
</tr>
<tr>
<td><code>[-cert-ca]</code> and <code>[-cert-serial]</code> or <code>[-cert-common-name]</code></td>
<td>The server certificate details of the service provider host (ONTAP system).</td>
<td></td>
</tr>
<tr>
<td><code>-verify-metadata-server</code></td>
<td>Whether the identity of the IdP metadata server must be validated (true or false). The best practice is to always set this value to true.</td>
<td></td>
</tr>
</tbody>
</table>
Creating login accounts

You can enable local or remote cluster and SVM administrator accounts. A local account is one in which the account information, public key, or security certificate resides on the storage system. AD account information is stored on a domain controller. LDAP and NIS accounts reside on LDAP and NIS servers.

Cluster and SVM administrators

A cluster administrator accesses the admin SVM for the cluster. The admin SVM and a cluster administrator with the reserved name admin are automatically created when the cluster is set up.

A cluster administrator with the default admin role can administer the entire cluster and its resources. The cluster administrator can create additional cluster administrators with different roles as needed.

An SVM administrator accesses a data SVM. The cluster administrator creates data SVMs and SVM administrators as needed.

SVM administrators are assigned the vsadmin role by default. The cluster administrator can assign different roles to SVM administrators as needed.

Merged roles

If you enable multiple remote accounts for the same user, the user is assigned the union of all roles specified for the accounts. That is, if an LDAP or NIS account is assigned the vsadmin role, and the AD group account for the same user is assigned the vsadmin-volume role, the AD user logs in with the more inclusive vsadmin capabilities. The roles are said to be merged.

Choices

- Enabling local account access on page 14
- Enabling Active Directory account access on page 18
- Enabling LDAP or NIS account access on page 19
- Configuring SAML authentication on page 20

Enabling local account access

A local account is one in which the account information, public key, or security certificate resides on the storage system. You can use the security login create command to enable local accounts to access an admin or data SVM.

Choices

- Enabling password account access on page 15
- Enabling SSH public key accounts on page 15
- Enabling SSH multifactor authentication (MFA) on page 16
- Enabling SSL certificate accounts on page 17
Enabling password account access

You can use the `security login create` command to enable administrator accounts to access an admin or data SVM with a password. You are prompted for the password after you enter the command.

Before you begin

You must be a cluster administrator to perform this task.

About this task

If you are unsure of the access control role that you want to assign to the login account, you can use the `security login modify` command to add the role later.

Modifying the role assigned to an administrator on page 22

Step

1. Enable local administrator accounts to access an SVM using a password:

```bash
security login create -vserver SVM_name -user-or-group-name user_or_group_name -application application -authmethod authentication_method -role role -comment comment
```

For complete command syntax, see the worksheet.

Creating or modifying login accounts on page 6

Example

The following command enables the cluster administrator account `admin1` with the predefined `backup` role to access the admin SVM `engCluster` using a password. You are prompted for the password after you enter the command.

```bash
cluster1::>security login create -vserver engCluster -user-or-group-name admin1 -application ssh -authmethod password -role backup
```

Enabling SSH public key accounts

You can use the `security login create` command to enable administrator accounts to access an admin or data SVM with an SSH public key.

Before you begin

You must be a cluster administrator to perform this task.

About this task

- You must associate the public key with the account before the account can access the SVM.
  
  Associating a public key with a user account on page 27

  You can perform this task before or after you enable account access.

- If you are unsure of the access control role that you want to assign to the login account, you can use the `security login modify` command to add the role later.
  
  Modifying the role assigned to an administrator on page 22

Step

1. Enable local administrator accounts to access an SVM using an SSH public key:
security login create -vserver SVM_name -user-or-group-name user_or_group_name -application application -authmethod authentication_method -role role -comment comment

For complete command syntax, see the worksheet.

Creating or modifying login accounts on page 6

Example

The following command enables the SVM administrator account svmadmin1 with the predefined vsadmin-volume role to access the SVM engData1 using an SSH public key:

```
cluster1::> security login create -vserver engData1 -user-or-group-name svmadmin1 -application ssh -authmethod publickey -role vsadmin-volume
```

After you finish

If you have not associated a public key with the administrator account, you must do so before the account can access the SVM.

Associating a public key with a user account on page 27

Enabling SSH multifactor authentication (MFA)

Starting with ONTAP 9.3, you can use the security login create command to enhance security by requiring that administrators log in to an admin or data SVM with both an SSH public key and a user password.

Before you begin

You must be a cluster administrator to perform this task.

About this task

- You must associate the public key with the account before the account can access the SVM.  
  Associating a public key with a user account on page 27
- You can perform this task before or after you enable account access.
- If you are unsure of the access control role that you want to assign to the login account, you can use the security login modify command to add the role later.  
  Modifying the role assigned to an administrator on page 22
- The user is always authenticated with public key authentication followed by password authentication.

Step

1. Require local administrator accounts to access an SVM using SSH MFA:

```
security login create -vserver SVM -user-or-group-name user_name -application ssh -authentication-method password|publickey -role admin -second-authentication-method password|publickey
```

Example

The following command requires the SVM administrator account admin2 with the predefined admin role to log in to the SVM engData1 with both an SSH public key and a user password:

```
cluster-1::> security login create -vserver engData1 -user-or-group-name admin2 -application ssh -authentication-method publickey -role admin -second-authentication-method password
```
Please enter a password for user 'admin2':
Please enter it again:
Warning: To use public-key authentication, you must create a public key for user "admin2".

After you finish
If you have not associated a public key with the administrator account, you must do so before the account can access the SVM.

Associating a public key with a user account on page 27

Enabling SSL certificate accounts
You can use the security login create command to enable administrator accounts to access an admin or data SVM with an SSL certificate.

Before you begin
You must be a cluster administrator to perform this task.

About this task
• You must install a CA-signed server digital certificate before the account can access the SVM.
  Generating and installing a CA-signed server certificate on page 28
You can perform this task before or after you enable account access.
• If you are unsure of the access control role you want to assign to the login account, you can add the role later with the security login modify command.
  Modifying the role assigned to an administrator on page 22

Note: For cluster administrator accounts, certificate authentication is supported only with the http and ontapi applications. For SVM administrator accounts, certificate authentication is supported only with the ontapi application.

Step
1. Enable local administrator accounts to access an SVM using an SSL certificate:

security login create -vserver SVM_name -user-or-group-name user_or_group_name -application application -authmethod authentication_method -role role -comment comment

For complete command syntax, see the worksheet.

Creating or modifying login accounts on page 6

Example
The following command enables the SVM administrator account svmadmin2 with the default vsadmin role to access the SVM engData2 using an SSL digital certificate.

cluster1::>security login create -vserver engData2 -user-or-group-name svmadmin2 -application ontapi -authmethod cert

After you finish
If you have not installed a CA-signed server digital certificate, you must do so before the account can access the SVM.

Generating and installing a CA-signed server certificate on page 28
Enabling Active Directory account access

You can use the `security login create` command to enable Active Directory (AD) user or group accounts to access an admin or data SVM. Any user in the AD group can access the SVM with the role that is assigned to the group.

Before you begin

- The cluster time must be synchronized to within five minutes of the time on the AD domain controller.
- You must be a cluster administrator to perform this task.

About this task

- You must configure AD domain controller access to the cluster or SVM before the account can access the SVM.
  
  ![Configuring Active Directory domain controller access on page 30](image)

- If you are unsure of the access control role that you want to assign to the login account, you can use the `security login modify` command to add the role later.
  
  ![Modifying the role assigned to an administrator on page 22](image)

  **Note:** AD group account access is supported only with the SSH and Ontapi applications.

Step

1. Enable AD user or group administrator accounts to access an SVM:

   ```
   security login create -vserver SVM_name -user-or-group-name user_or_group_name -application application -authmethod domain -role role -comment comment
   ```

   For complete command syntax, see the worksheet.

   ![Creating or modifying login accounts on page 6](image)

   **Example**

   The following command enables the AD cluster administrator account `DOMAIN1\guest1` with the predefined `backup` role to access the admin SVM `engCluster`.

   ```
   cluster1::>security login create -vserver engCluster -user-or-group-name DOMAIN1\guest1 -application ssh -authmethod domain -role backup
   ```

   The following command enables the SVM administrator accounts in the AD group account `DOMAIN1\adgroup` with the predefined `vsadmin-volume` role to access the SVM `engData`.

   ```
   cluster1::>security login create -vserver engData -user-or-group-name DOMAIN1\adgroup -application ssh -authmethod domain -role vsadmin-volume
   ```

After you finish

If you have not configured AD domain controller access to the cluster or SVM, you must do so before the account can access the SVM.

![Configuring Active Directory domain controller access on page 30](image)
Enabling LDAP or NIS account access

You can use the `security login create` command to enable LDAP or NIS user accounts to access an admin or data SVM. If you have not configured LDAP or NIS server access to the SVM, you must do so before the account can access the SVM.

Before you begin

You must be a cluster administrator to perform this task.

About this task

- Group accounts are not supported.
- You must configure LDAP or NIS server access to the SVM before the account can access the SVM.
  
  Configuring LDAP or NIS server access on page 32

  You can perform this task before or after you enable account access.

- If you are unsure of the access control role that you want to assign to the login account, you can use the `security login modify` command to add the role later.
  
  Modifying the role assigned to an administrator on page 22

- Beginning with ONTAP 9.4, multifactor authentication (MFA) is supported for remote users over LDAP or NIS servers.

Steps

1. Enable LDAP or NIS user or group accounts to access an SVM:

   ```
   security login create -vserver SVM_name -user-or-group-name user_name -application application -authmethod nsswitch -role role -comment comment -is-ns-switch-group yes|no
   ```

   For complete command syntax, see the worksheet.
   
   Creating or modifying login accounts on page 6

   Example

   The following command enables the LDAP or NIS cluster administrator account `guest2` with the predefined `backup` role to access the admin SVM `engCluster`.

   ```
   cluster1::>security login create -vserver engCluster -user-or-group-name guest2 -application ssh -authmethod nsswitch -role backup
   ```

2. Enable MFA login for LDAP or NIS users:

   ```
   security login modify -user-or-group-name rem_usr1 -application ssh -authentication-method nsswitch -role admin -is-ns-switch-group no -second-authentication-method publickey
   ```

   The authentication method can be specified as `publickey` and second authentication method as `nsswitch`.

   Example

   The following example shows the MFA authentication being enabled:

   ```
   cluster-1::*> security login modify -user-or-group-name rem_usr2 -application ssh -authentication-method nsswitch -vserver cluster-1 -second-authentication-method publickey
   ```
After you finish

If you have not configured LDAP or NIS server access to the SVM, you must do so before the account can access the SVM.

Configuring LDAP or NIS server access on page 32

Configuring SAML authentication

Starting with ONTAP 9.3, you can configure Security Assertion Markup Language (SAML) authentication for web services. When SAML authentication is configured and enabled, users are authenticated by an external Identity Provider (IdP) instead of the directory service providers such as Active Directory and LDAP.

Before you begin

• You must have configured the IdP for SAML authentication.
• You must have the IdP URI.

About this task

• SAML authentication applies only to the http and ontapi applications.
  The http and ontapi applications are used by the following web services: Service Processor Infrastructure, ONTAP APIs, or OnCommand System Manager.
• SAML authentication is applicable only for accessing the admin SVM.

Steps

1. Create a SAML configuration so that ONTAP can access the IdP metadata:

   ```
   security saml-sp create -idp-uri idp_uri -sp-host ontap_host_name
   ```

   `idp_uri` is the FTP or HTTP address of the IdP host from where the IdP metadata can be downloaded.

   `ontap_host_name` is the host name or IP address of the SAML service provider host, which in this case is the ONTAP system. By default, the IP address of the cluster-management LIF is used.

   You can optionally provide the ONTAP server certificate information. By default, the ONTAP web server certificate information is used.

Example

```bash

Warning: This restarts the web server. Any HTTP/S connections that are active will be disrupted.
Do you want to continue? [y|n]: y
[Job 179] Job succeeded: Access the SAML SP metadata using the URL: https://10.63.56.150/saml-sp/Metadata
```

Configure the IdP and Data ONTAP users for the same directory server domain to ensure that users are the same for different authentication methods. See the "security login show" command for the Data ONTAP user configuration.
The URL to access the ONTAP host metadata is displayed.

2. From the IdP host, configure the IdP with the ONTAP host metadata.
   For more information about configuring the IdP, see the IdP documentation.

3. Enable SAML configuration:
   
   `security saml-sp modify -is-enabled true`
   
   Any existing user that accesses the `http` or `ontapi` application is automatically configured for SAML authentication.

4. If you want to create users for the `http` or `ontapi` application after SAML is configured, specify SAML as the authentication method for the new users.
   
   a. Create a login method for new users with SAML authentication:
      
      `security login create -user-or-group-name user_name -application [http | ontapi] -authentication-method saml -vserver svm_name`
      
      Example
      
      `cluster_12::> security login create -user-or-group-name admin1 -application http -authentication-method saml -vserver cluster_12`
      
      b. Verify that the user entry is created:
         
         `security login show`
         
         Example
         
         `cluster_12::> security login show`

Related information

ONTAP 9 commands
Managing access-control roles

The role assigned to an administrator determines the commands to which the administrator has access. You assign the role when you create the account for the administrator. You can assign a different role or define custom roles as needed.

Related concepts

- *Predefined roles for cluster administrators* on page 24
- *Predefined roles for SVM administrators* on page 24

Related tasks

- *Modifying the role assigned to an administrator* on page 22
- *Defining custom roles* on page 23

Modifying the role assigned to an administrator

You can use the `security login modify` command to change the role of a cluster or SVM administrator account. You can assign a predefined or custom role.

**Before you begin**

You must be a cluster administrator to perform this task.

**Step**

1. Change the role of a cluster or SVM administrator:

   ```
   security login modify -vserver SVM_name -user-or-group-name user_or_group_name -application application -authmethod authentication_method -role role -comment comment
   ```

   For complete command syntax, see the worksheet.

   *Creating or modifying login accounts* on page 6

   **Example**

   The following command changes the role of the AD cluster administrator account `DOMAIN1\guest1` to the predefined `readonly` role.

   ```
   cluster1::>security login modify -vserver engCluster -user-or-group-name DOMA1\guest1 -application ssh -authmethod domain -role readonly
   ```

   The following command changes the role of the SVM administrator accounts in the AD group account `DOMAIN1\adgroup` to the custom `vol_role` role.

   ```
   cluster1::>security login modify -vserver engData -user-or-group-name DOMA1\adgroup -application ssh -authmethod domain -role vol_role
   ```
Defining custom roles

You can use the `security login role create` command to define a custom role. You can execute the command as many times as necessary to achieve the exact combination of capabilities that you want to associate with the role.

Before you begin

You must be a cluster administrator to perform this task.

About this task

- A role, whether predefined or custom, grants or denies access to ONTAP commands or command directories.
  A command directory (**volume**, for example) is a group of related commands and command subdirectories. Except as described in this procedure, granting or denying access to a command directory grants or denies access to each command in the directory and its subdirectories.
- Specific command access or subdirectory access overrides parent directory access.
  If a role is defined with a command directory, and then is defined again with a different access level for a specific command or for a subdirectory of the parent directory, the access level that is specified for the command or subdirectory overrides that of the parent.

Note: You cannot assign an SVM administrator a role that gives access to a command or command directory that is available only to the **admin** cluster administrator—for example, the `security` command directory.

Step

1. Define a custom role:

   ```
   security login role create -vserver SVM_name -role role -cmddirname command_or_directory_name -access access_level -query query
   ```

   For complete command syntax, see the worksheet.

   *Defining custom roles on page 7*

Example

The following commands grant the **vol_role** role full access to the commands in the **volume** command directory and read-only access to the commands in the **volume snapshot** subdirectory.

```
cluster1::>security login role create -role vol_role -cmddirname "volume" -access all
cluster1::>security login role create -role vol_role -cmddirname "volume snapshot" -access readonly
```

The following commands grant the **SVM_storage** role read-only access to the commands in the **storage** command directory, no access to the commands in the **storage encryption** subdirectory, and full access to the **storage aggregate plex offline** nonintrinsic command.

```
cluster1::>security login role create -role SVM_storage -cmddirname "storage" -access readonly
cluster1::>security login role create -role SVM_storage -cmddirname "storage encryption" -access none
```
Predefined roles for cluster administrators

The predefined roles for cluster administrators should meet most of your needs. You can create custom roles as necessary. By default, a cluster administrator is assigned the predefined `admin` role.

The following table lists the predefined roles for cluster administrators:

<table>
<thead>
<tr>
<th>This role...</th>
<th>Has this level of access...</th>
<th>To the following commands or command directories</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>all</td>
<td>All command directories (DEFAULT)</td>
</tr>
<tr>
<td>autosupport</td>
<td>all</td>
<td>• set</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• system node autosupport</td>
</tr>
<tr>
<td></td>
<td>none</td>
<td>All other command directories (DEFAULT)</td>
</tr>
<tr>
<td>backup</td>
<td>all</td>
<td>vserver services ndmp</td>
</tr>
<tr>
<td></td>
<td>readonly</td>
<td>volume</td>
</tr>
<tr>
<td></td>
<td>none</td>
<td>All other command directories (DEFAULT)</td>
</tr>
<tr>
<td>readonly</td>
<td>all</td>
<td>• security login password</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• set</td>
</tr>
<tr>
<td></td>
<td>none</td>
<td>security</td>
</tr>
<tr>
<td></td>
<td>readonly</td>
<td>All other command directories (DEFAULT)</td>
</tr>
<tr>
<td>none</td>
<td>none</td>
<td>All command directories (DEFAULT)</td>
</tr>
</tbody>
</table>

Note: The `autosupport` role is assigned to the predefined `autosupport` account, which is used by AutoSupport OnDemand. ONTAP prevents you from modifying or deleting the `autosupport` account. ONTAP also prevents you from assigning the `autosupport` role to other user accounts.

Predefined roles for SVM administrators

The predefined roles for SVM administrators should meet most of your needs. You can create custom roles as necessary. By default, an SVM administrator is assigned the predefined `vsadmin` role.

The following table lists the predefined roles for SVM administrators:
<table>
<thead>
<tr>
<th>Role name</th>
<th>Capabilities</th>
</tr>
</thead>
</table>
| vsadmin         | • Managing own user account local password and key information  
                  • Managing volumes, except volume moves  
                  • Managing quotas, qtrees, Snapshot copies, and files  
                  • Managing LUNs  
                  • Performing SnapLock operations, except privileged delete  
                  • Configuring protocols: NFS, CIFS, iSCSI, and FC, including FCoE  
                  • Configuring services: DNS, LDAP, and NIS  
                  • Monitoring jobs  
                  • Monitoring network connections and network interface  
                  • Monitoring the health of the SVM                                                                                                    |
| vsadmin-volume  | • Managing own user account local password and key information  
                  • Managing volumes, including volume moves  
                  • Managing quotas, qtrees, Snapshot copies, and files  
                  • Managing LUNs  
                  • Configuring protocols: NFS, CIFS, iSCSI, and FC, including FCoE  
                  • Configuring services: DNS, LDAP, and NIS  
                  • Monitoring network interface  
                  • Monitoring the health of the SVM                                                                                            |
| vsadmin-protocol| • Managing own user account local password and key information  
                  • Configuring protocols: NFS, CIFS, iSCSI, and FC, including FCoE  
                  • Configuring services: DNS, LDAP, and NIS  
                  • Managing LUNs  
                  • Monitoring network interface  
                  • Monitoring the health of the SVM                                                                                                    |
| vsadmin-backup  | • Managing own user account local password and key information  
                  • Managing NDMP operations  
                  • Making a restored volume read/write  
                  • Managing SnapMirror relationships and Snapshot copies  
                  • Viewing volumes and network information                                                                                       |
| vsadmin-snaplock| • Managing own user account local password and key information  
                  • Managing volumes, except volume moves  
                  • Managing quotas, qtrees, Snapshot copies, and files  
                  • Performing SnapLock operations, including privileged delete  
                  • Configuring protocols: NFS and CIFS  
                  • Configuring services: DNS, LDAP, and NIS  
                  • Monitoring jobs  
                  • Monitoring network connections and network interface                                                                                   |
<table>
<thead>
<tr>
<th>Role name</th>
<th>Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsadmin-readonly</td>
<td>• Managing own user account local password and key information</td>
</tr>
<tr>
<td></td>
<td>• Monitoring the health of the SVM</td>
</tr>
<tr>
<td></td>
<td>• Monitoring network interface</td>
</tr>
<tr>
<td></td>
<td>• Viewing volumes and LUNs</td>
</tr>
<tr>
<td></td>
<td>• Viewing services and protocols</td>
</tr>
</tbody>
</table>
Managing administrator accounts

Depending on how you have enabled account access, you may need to associate a public key with a local account, install a CA-signed server digital certificate, or configure AD, LDAP, or NIS access. You can perform all of these tasks before or after enabling account access.

Related tasks

- Associating a public key with an administrator account on page 27
- Generating and installing a CA-signed server certificate on page 28
- Configuring Active Directory domain controller access on page 30
- Configuring LDAP or NIS server access on page 32
- Changing an administrator password on page 34
- Locking and unlocking an administrator account on page 35

Associating a public key with an administrator account

For SSH public key authentication, you must associate the public key with an administrator account before the account can access the SVM. You can use the `security login publickey create` command to associate a key with an administrator account.

Before you begin

- You must have generated the SSH key.
- You must be a cluster or SVM administrator to perform this task.

About this task

If you authenticate an account over SSH with both a password and an SSH public key, the account is authenticated first with the public key.

Step

1. Associate a public key with an administrator account:

   `security login publickey create -vserver SVM_name -username user_name -index index -publickey certificate -comment comment`

   For complete command syntax, see the worksheet.

   Example

   The following command associates a public key with the SVM administrator account `svmadmin1` for the SVM `engData1`. The public key is assigned index number 5.

   ```bash
   cluster1::>security login publickey create -vserver engData1 -username svmadmin1 -index 5 -publickey "ssh-rsa AAAAB3NzaC1yc2EAAAABIBAwAAAIEAspH64CYbUsDQCdW22JnK6J/vU9upnKzd2zAk9C1f7YaW RUAPNs2Qe51UmQ31di8AD0Vfbr5T6HZPCixNAIzaFciiDy7hgmndj9eNGedGzr/JNRfTBQBD1h2ybX+72DpqB0tYWBhe6eDji0PLobZBGmIPXhBVjeU44i7W4+s0hGGE=tsmith@publickey.example.com"
   ```
Generating and installing a CA-signed server certificate

On production systems, it is a best practice to install a CA-signed digital certificate for use in authenticating the cluster or SVM as an SSL server. You can use the `security certificate generate-csr` command to generate a certificate signing request (CSR), and the `security certificate install` command to install the certificate you receive back from the certificate authority.

Related tasks

- Generating a certificate signing request on page 28
- Installing a CA-signed server certificate on page 29

Generating a certificate signing request

You can use the `security certificate generate-csr` command to generate a certificate signing request (CSR). After processing your request, the certificate authority (CA) sends you the signed digital certificate.

Before you begin

You must be a cluster or SVM administrator to perform this task.

Steps

1. Generate a CSR:

   ```
   security certificate generate-csr -common-name FQDN_or_common_name -size 512|1024|1536|2048 -country country -state state -locality locality -organization organization -unit unit -email-addr email_of_contact -hash-function SHA1|SHA256|MD5
   ```

   Example

   The following command creates a CSR with a 2048-bit private key generated by the SHA256 hashing function for use by the Software group in the IT department of a company whose custom common name is `server1.companyname.com`, located in Sunnyvale, California, USA. The email address of the SVM contact administrator is `web@example.com`. The system displays the CSR and the private key in the output.

   ```
   cluster1::>security certificate generate-csr -common-name server1.companyname.com -size 2048 -country US -state California -locality Sunnyvale -organization IT -unit Software -email-addr web@example.com -hash-function SHA256
   ```

   Certificate Signing Request :
   ```plaintext
   -----BEGIN CERTIFICATE REQUEST-----
   MIIBGjCBxQIBAdBgQIQCQMCgAwEwYDVQQDEwtleGFtcGxlLmNvbTBMAgEBBCByBggC
   -----END CERTIFICATE REQUEST-----
   ```

   Private Key :
   ```plaintext
   -----BEGIN RSA PRIVATE KEY-----
   MIIBDjAEBAAAJBAPXFanNoJApTlnzSxOcxixqImlRk2CR7tVmTYqPSvWhVtwDjBm
   -----END RSA PRIVATE KEY-----
   ```
Note: Please keep a copy of your certificate request and private key for future reference.

2. Copy the certificate request from the CSR output, and send it in electronic form (such as email) to a trusted third-party CA for signing.

After processing your request, the CA sends you the signed digital certificate. You should keep a copy of the private key and the CA-signed digital certificate.

Installing a CA-signed server certificate

You can use the `security certificate install` command to install a CA-signed server certificate on an SVM. ONTAP prompts you for the certificate authority (CA) root and intermediate certificates that form the certificate chain of the server certificate.

Before you begin

You must be a cluster or SVM administrator to perform this task.

Step

1. Install a CA-signed server certificate:

   ```
   security certificate install -vserver SVM_name -type certificate_type
   ```

   For complete command syntax, see the worksheet.

   **Installing a CA-signed server digital certificate** on page 9

   **Note:** ONTAP prompts you for the CA root and intermediate certificates that form the certificate chain of the server certificate. The chain starts with the certificate of the CA that issued the server certificate, and can range up to the root certificate of the CA. Any missing intermediate certificates result in the failure of server certificate installation.

   **Example**

   The following command installs the CA-signed server certificate and intermediate certificates on the SVM `engData2`.

   ```
   cluster1::>security certificate install -vserver engData2 -type server
   Please enter Certificate: Press <Enter> when done
   -----BEGIN CERTIFICATE-----
   MIIB8TCCAuzgAwIBAgIBADANBgkqhkiG9w0BAQEFADBfMRMwEQYDVQQDEwpuZXRhcHAvY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQLBAoTADEJMAcGA1UECxMAMQ8wDQYJKoZIhvcNAQkBFgAwHbNAhcNMTAwNDI2MTk0OTI4WhcNMTAwNDI2MTk0OTI4
   -----END CERTIFICATE-----
   Please enter Private Key: Press <Enter> when done
   -----BEGIN RSA PRIVATE KEY-----
   MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gkOBPX+Y5MLycaUdXAhv7XhumHNPvF
   C61X2G3Z8y8e1alh9t4x+v0Eozq+UaqH1t0CAwEAAQJBAMZjDdWgmlm3iQ/r/n8VT
   PFNnZnhvCVX70tbUaUgPkw+QCC9h9dP1JmuQKeDr+wUMWkn1DEgrf1lpzfJGhrLJ
   z7UCiQD8d3gQO6JryX+RbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwihxANq99SsuS18U
   DiPvedaKTj6+EcuXFCXz+G0rfGT2K8uzAiEAr1mnrzfYC8kwE9k7A0y1Rz璧HdpWk9
   AvudJn/+z+H1BD0CIQQD93P/xpaJETNZ53Au49VE5Jba/Jugckrbdos/1Sd7nQ1s
   aEMAzt6qHHT4mnd18Bo8sDgedG2SKx6Qbn21pNuZ7rc=
   ```
-----END RSA PRIVATE KEY-----

Do you want to continue entering root and/or intermediate certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIE+zCCBGSgAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1Zh
bGlDZXJ0IFZhbGlkYXRpb24gTmV0d29yazEXMBUxAUEChMVfewZaUNicnQsIElu
Yy4wMTAwMHYwczQwMQswCQg3MjUxMjMxMy0xNy0wNzowMjEgMjUzMDkxMC4xMBQw
-----END CERTIFICATE-----

Do you want to continue entering root and/or intermediate certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1Zh
bGlDZXJ0IFZhbGlkYXRpb24gTmV0d29yazEXMBUxAUEChMVfewZaUNicnQsIElu
Yy4wMTAwMHYwczQwMQswCQg3MjUxMjMxMy0xNy0wNzowMjEgMjUzMDkxMC4xMBQw
-----END CERTIFICATE-----

Do you want to continue entering root and/or intermediate certificates {y|n}: n

You should keep a copy of the private key and the CA-signed digital certificate for future reference.

Configuring Active Directory domain controller access

You must configure AD domain controller access to the cluster or SVM before an AD account can access the SVM. If you have already configured a CIFS server for a data SVM, you can configure the SVM as a gateway, or tunnel, for AD access to the cluster. If you have not configured a CIFS server, you can create a computer account for the SVM on the AD domain.

Choices

• Configuring an authentication tunnel on page 30
• Creating an SVM computer account on the domain on page 31

Configuring an authentication tunnel

If you have already configured a CIFS server for a data SVM, you can use the security login domain-tunnel create command to configure the SVM as a gateway, or tunnel, for AD access to the cluster.

Before you begin

• You must have configured a CIFS server for a data SVM.
• You must have enabled an AD domain user account to access the admin SVM for the cluster.
• You must be a cluster administrator to perform this task.
Step

1. Configure a CIFS-enabled data SVM as an authentication tunnel for AD domain controller access to the cluster:

   ```bash
   security login domain-tunnel create -vserver SVM_name
   ```

   For complete command syntax, see the worksheet.

   *Configuring Active Directory domain controller access* on page 10

   **Note:** The SVM must be running for the user to be authenticated.

   **Example**

   The following command configures the CIFS-enabled data SVM *engData* as an authentication tunnel.

   ```bash
   cluster1::>security login domain-tunnel create -vserver engData
   ```

### Creating an SVM computer account on the domain

If you have not configured a CIFS server for a data SVM, you can use the `vserver active-directory create` command to create a computer account for the SVM on the domain.

**Before you begin**

You must be a cluster or SVM administrator to perform this task.

**About this task**

After you enter the `vserver active-directory create` command, you are prompted to provide the credentials for an AD user account with sufficient privileges to add computers to the specified organizational unit in the domain. The password of the account cannot be empty.

**Step**

1. Create a computer account for an SVM on the AD domain:

   ```bash
   vserver active-directory create -vserver SVM_name -account-name NetBIOS_account_name -domain domain -ou organizational_unit
   ```

   For complete command syntax, see the worksheet.

   *Configuring Active Directory domain controller access* on page 10

   **Example**

   The following command creates a computer account named *ADSERVER1* on the domain *example.com* for the SVM *engData*. You are prompted to enter the AD user account credentials after you enter the command.

   ```bash
   cluster1::>vserver active-directory create -vserver engData -account-name ADSERVER1 -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: Administrator

   Enter the password:
Configuring LDAP or NIS server access

You must configure LDAP or NIS server access to an SVM before LDAP or NIS accounts can access the SVM. The switch feature lets you use LDAP or NIS as alternative name service sources.

Related tasks
- Configuring LDAP server access on page 32
- Configuring NIS server access on page 33
- Creating a name service switch on page 34

Configuring LDAP server access

You must configure LDAP server access to an SVM before LDAP accounts can access the SVM. You can use the `vserver services name-service ldap client create` command to create an LDAP client configuration on the SVM. You can then use the `vserver services name-service ldap create` command to associate the LDAP client configuration with the SVM.

Before you begin
- You must have installed a CA-signed server digital certificate on the SVM.
- You must be a cluster or SVM administrator to perform this task.

About this task

Most LDAP servers can use the default schemas provided by ONTAP:
- AD-IDMU (Windows 2008, Windows 2012 and later AD servers)
- AD-SFU (Windows 2003 and earlier AD servers)
- RFC-2307 (UNIX LDAP servers)

It is best to use the default schemas unless there is a requirement to do otherwise. If so, you can create your own schema by copying a default schema and modifying the copy. For more information, see the NFS Configuration Power Guide.

Steps

1. Create an LDAP client configuration on an SVM:

   ```bash
   vserver services name-service ldap client create -vserver SVM_name -client-config client_configuration -servers LDAP_server_IPs -schema schema -use-start-tls true|false
   ```

   **Note:** Start TLS is supported for access to data SVMs only. It is not supported for access to admin SVMs.

   For complete command syntax, see the worksheet.

Example

The following command creates an LDAP client configuration named `corp` on the SVM `engData`. The client makes anonymous binds to the LDAP servers with the IP addresses `172.160.0.100` and `172.16.0.101`. The client uses the `RFC-2307` schema to make LDAP queries. Communication between the client and server is encrypted using Start TLS.
2. Associate the LDAP client configuration with the SVM:

```
cluster1::> vserver services name-service ldap create -vserver SVM_name -client-config client_configuration -client-enabled true|false
```

For complete command syntax, see the worksheet. 

*Configuring LDAP or NIS server access* on page 11

**Example**

The following command associates the LDAP client configuration `corp` with the SVM `engData`, and enables the LDAP client on the SVM.

```
cluster1::> vserver services name-service ldap create -vserver engData -client-config corp -client-enabled true
```

*Note:* Starting in ONTAP 9.2, the `vserver services name-service ldap create` command performs an automatic configuration validation and reports an error message if ONTAP is unable to contact the name server.

3. Validate the status of the name servers by using the `vserver services name-service ldap check` command.

The following command validates LDAP servers on the SVM `vs0`.

**Example**

```
cluster1::> vserver services name-service ldap check -vserver vs0
```

The name service check command is available starting in ONTAP 9.2.

---

### Configuring NIS server access

You must configure NIS server access to an SVM before NIS accounts can access the SVM. You can use the `vserver services name-service nis-domain create` command to create an NIS domain configuration on an SVM.

**Before you begin**

- All configured servers must be available and accessible before you configure the NIS domain on the SVM.
- You must be a cluster or SVM administrator to perform this task.

**About this task**

You can create multiple NIS domains. Only one NIS domain can be set to **active** at a time.
Step

1. Create an NIS domain configuration on an SVM:

   ```bash
   vserver services name-service nis-domain create -vserver SVM_name -domain client_configuration -active true|false -nis-servers NIS_server_IPs
   ```

   For complete command syntax, see the worksheet.

   Configuring LDAP or NIS server access on page 11

   **Note:** Starting in ONTAP 9.2, the field `-nis-servers` replaces the field `-servers`. This new field can take either a hostname or an IP address for the NIS server.

Example

The following command creates an NIS domain configuration on the SVM `engData`. The NIS domain `nisdomain` is active on creation and communicates with an NIS server with the IP address `192.0.2.180`.

```bash
cluster1::>vserver services name-service nis-domain create -vserver engData -domain nisdomain -active true -nis-servers 192.0.2.180
```

Creating a name service switch

The name service switch feature lets you use LDAP or NIS as alternative name service sources. You can use the `vserver services name-service ns-switch modify` command to specify the look-up order for name service sources.

Before you begin

- You must have configured LDAP and NIS server access.
- You must be a cluster administrator or SVM administrator to perform this task.

Step

1. Specify the lookup order for name service sources:

   ```bash
   vserver services name-service ns-switch modify -vserver SVM_name -database name_service_switch_database -sources name_service_source_order
   ```

   For complete command syntax, see the worksheet.

   Configuring LDAP or NIS server access on page 11

Example

The following command specifies the lookup order of the LDAP and NIS name service sources for the `passwd` database on the `engData` SVM.

```bash
cluster1::>vserver services name-service ns-switch modify -vserver engData -database passwd -source files ldap,nis
```

Changing an administrator password

You should change your initial password immediately after logging into the system for the first time. If you are an SVM administrator, you can use the `security login password` command to
change your own password. If you are a cluster administrator, you can use the `security login password` command to change any administrator's password.

**Before you begin**
- You must be a cluster or SVM administrator to change your own password.
- You must be a cluster administrator to change another administrator's password.

**About this task**
The new password must observe the following rules:
- It cannot contain the user name
- It must be at least eight characters long
- It must contain at least one letter and one number
- It cannot be the same as the last six passwords

*Note:* You can use the `security login role config modify` command to modify the password rules for accounts associated with a given role. For more information, see the man page.

```bash
security login role config modify
```

**Step**

1. Change an administrator password:
   ```bash
   security login password -vserver SVM_name -username user_name
   ```

   **Example**
The following command changes the password of the administrator `admin1` for the SVM `vs1.example.com`. You are prompted to enter the current password, then enter and reenter the new password.

   ```bash
   vs1.example.com::>security login password -vserver engData -username admin1
   Please enter your current password:
   Please enter a new password:
   Please enter it again:
   ```

**Locking and unlocking an administrator account**
You can use the `security login lock` command to lock an administrator account, and the `security login unlock` command to unlock the account.

**Before you begin**
You must be a cluster administrator to perform these tasks.

**Steps**

1. Lock an administrator account:
   ```bash
   security login lock -vserver SVM_name -username user_name
   ```

   **Example**
The following command locks the administrator account `admin1` for the SVM `vs1.example.com`:

   ```bash
   vs1.example.com::>security login lock -vserver engData -username admin1
   ```
2. Unlock an administrator account:

   security login unlock -vserver SVM_name -username user_name

   Example

   The following command unlocks the administrator account admin1 for the SVM vs1.example.com:

   cluster1::>security login unlock -vserver engData -username admin1

Managing failed login attempts

Repeated failed login attempts sometimes indicate that an intruder is attempting to access the storage system. You can take a number of steps to ensure that an intrusion does not take place.

How you will know that login attempts have failed

The Event Management System (EMS) notifies you about failed login attempts every hour. You can find a record of failed login attempts in the audit.log file.

What to do if repeated login attempts fail

In the short term, you can take a number of steps to prevent an intrusion:

- Require that passwords be composed of a minimum number of uppercase characters, lowercase characters, special characters, and/or digits
- Impose a delay after a failed login attempt
- Limit the number of allowed failed login attempts, and lock out users after the specified number of failed attempts
- Expire and lock out accounts that are inactive for a specified number of days

You can use the security login role config modify command to perform these tasks.

Over the long term, you can take these additional steps:

- Use the security ssh modify command to limit the number of failed login attempts for all newly created SVMs.
- Migrate existing MD5-algorithm accounts to the more secure SHA-512 algorithm by requiring users to change their passwords.

Related tasks

Enforcing SHA-2 on administrator account passwords on page 36

Enforcing SHA-2 on administrator account passwords

Administrator accounts created prior to ONTAP 9.0 continue to use MD5 passwords after the upgrade, until the passwords are manually changed. MD5 is less secure than SHA-2. Therefore, after
upgrading, you should prompt users of MD5 accounts to change their passwords to use the default SHA-512 hash function.

Steps

1. Migrate the MD5 administrator accounts to the SHA-512 password hash function:
   a. Expire all MD5 administrator accounts:
      \[\text{security login expire-password -vserver * -username * -hash-function md5}\]
      Doing so forces MD5 account users to change their passwords upon next login.
   b. Ask users of MD5 accounts to log in through a console or SSH session.
      The system detects that the accounts are expired and prompts users to change their passwords. SHA-512 is used by default for the changed passwords.

2. Optional: For MD5 accounts whose users do not log in to change their passwords within a period of time, force the account migration:
   a. Lock accounts that still use the MD5 hash function (advanced privilege level):
      \[\text{security login expire-password -vserver * -username * -hash-function md5 -lock-after integer}\]
      After the number of days specified by -lock-after, users cannot access their MD5 accounts.
   b. Unlock the accounts when the users are ready to change their passwords:
      \[\text{security login unlock -vserver vserver_name -username user_name}\]
   c. Have users log in to their accounts through a console or SSH session and change their passwords when the system prompts them to do so.
Where to find additional information

After you have enabled login accounts for ONTAP cluster and SVM administrators, you can perform more advanced tasks.

- **ONTAP 9 commands**
  Describes additional commands for enabling administrator account access and for using RBAC to define administrator capabilities.

- **Cluster management using System Manager**
  Describes how to use OnCommand System Manager to perform tasks related to administrator authentication and RBAC.

- **NetApp Documentation: OnCommand Workflow Automation (current releases)**
  Describes how to use the OnCommand Workflow Automation scripting tool to perform tasks related to administrator authentication and RBAC.

- **System administration**
  Describes general system administration for storage systems running ONTAP.
Trademark information

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

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.

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., 1395 Crossman Ave., Sunnyvale, CA 94089 U.S.
• Telephone: +1 (408) 822-6000
• Fax: +1 (408) 822-4501
• Support telephone: +1 (888) 463-8277
Index

A

about this guide

deciding whether to use the Administrator Authentication and RBAC Power Guide 4

access-control roles

introduction to managing 22

predefined roles for SVM administrators 24

predefined, for cluster administrators 24

access, AD domain controller

introduction to configuring access 30

access, cluster

configuring an AD authentication tunnel for 30

access, LDAP server

configuring 32

access, NIS server

configuring 33

access, server

introduction to configuring for LDAP or NIS 32

account passwords

enforcing SHA-2 on user 36

accounts, administrator

changing the login password 34

accounts, SSH public key

enabling local account access to SVMs 15

accounts, user

commands for installing a CA-signed server digital certificate 28

configuring an AD authentication tunnel 30

configuring LDAP server access 32

configuring NIS server access 33

generating a digital certificate signing request 28

installing a CA-signed server digital certificate 29

introduction to configuring Active Directory domain controller access 30

introduction to configuring LDAP access 32

introduction to configuring NIS access 32

Active Directory

configuring an authentication tunnel 30

creating an SVM computer account on the domain 31

enabling accounts for cluster administrators 18

enabling accounts for SVM administrators 18

introduction to configuring domain controller access 30

administrator accounts

changing the login password 34

locking and unlocking 35

administrator authentication

where to find additional information about 38

workflow for enabling 5

worksheets to gather configuration information 6

administrator accounts

associating a public key with an administrator account 27

administrators

predefined roles for cluster 24

predefined roles for SVM 24

audience

for the guide 4

authentication tunnels, AD configuring 30

C

CA-signed server digital certificates

commands for installing 28

installing 29

certificate signing requests, digital

generating 28

certificates, CA-signed server digital

commands for installing 28

installing 29

cluster access

configuring an AD authentication tunnel for 30

cluster administrators

predefined roles for 24

comments

how to send feedback about documentation 41

computer accounts, SVM

creating on the domain 31

configuring

SAML authentication 20

controller access, AD domain

introduction to configuring access 30

creating

Active Directory user accounts for cluster administrators 18

Active Directory user accounts for SVM administrators 18

local user account access to SVMs with an SSH public key 15

local user accounts for cluster administrators 14, 15, 17

local user accounts for SVM administrators 14, 15, 17

name service switches 34

D

data SVMs

configuring an AD authentication tunnel 30

introduction to configuring Active Directory domain controller access 30

digital certificate signing requests

generating 28

digital certificates, CA-signed server

commands for installing 28

installing 29

documentation

additional information about administrator authentication 38

how to receive automatic notification of changes to 41

how to send feedback about 41

domain controller access, AD

introduction to configuring access 30
domains
  creating an SVM computer account on 31

F
feedback
  how to send comments about documentation 41

I
information
  how to send feedback about improving documentation 41

K
key accounts, SSH public
  enabling local account access to SVMs 15

L
LDAP
  configuring server access 32
  creating name service switches 34
  enabling user accounts to access SVMs 19
  introduction to configuring server access 32
local users
  associating a public key with an administrator account 27
  commands for installing a CA-signed server digital certificate 28
  enabling accounts for cluster administrators 14, 15, 17
  enabling accounts for SVM administrators 14, 15, 17
  enabling accounts to access SVMs with an SSH public key 15
  generating a digital certificate signing request 28
  installing a CA-signed server digital certificate 29
locking
  administrator accounts 35
login accounts
  changing the password 34
  creating for SVM administrators 14

M
MD5
  enforcing SHA-2 on administrator account passwords 36
MFA
  See multifactor authentication
  modifying administrator roles 22
multifactor authentication
  by Identity Provider 20
  for local user accounts 16
  SAML 20
  using password and public key 16
  using SSH 16

N
name service switches
  creating 34
NIS
  configuring server access 33
  creating name service switches 34
  enabling user accounts to access SVMs 19
  introduction to configuring server access 32

P
passwords
  enforcing SHA-2 on administrator account 36
  passwords, user changing 34
power guides
  requirements for using this guide 4
  predefined roles
    for cluster administrators 24
    for SVM administrators 24
public key accounts, SSH
  enabling local account access to SVMs 15

R
RBAC
  defining custom roles 23
  managing access-control roles, introduction to 22
  modifying administrator roles 22
  predefined roles for cluster administrators 24
  predefined roles for SVM administrators 24
  workflow for enabling 5
RBAC configuration
  worksheets to gather configuration information 6
requests, digital certificate signing generating 28
role-based access control
  defining custom roles 23
  managing access-control roles, introduction to 22
  modifying administrator roles 22
  predefined roles for cluster administrators 24
  predefined roles for SVM administrators 24
roles
  introduction to managing access-control 22
  predefined for SVM administrators 24
  predefined, for cluster administrators 24

S
SAML authentication
  configuring 20
  creating 20
  enabling 20
security
  enforcing SHA-2 on administrator account passwords 36
server access
  introduction to configuring for LDAP or NIS 32
server access, LDAP
  configuring 32
server access, NIS
configuring server digital certificates, CA-signed commands for installing
installing SHA-2
enforcing on administrator account passwords signing requests, digital certificate generating
SSH
authentication using password and public key multifactor authentication
SSH public key accounts enabling local account access to SVMs storage systems preventing intrusions suggestions how to send feedback about documentation SVMs
associating a public key with an administrator account changing the account password commands for installing a CA-signed server digital certificate configuring an AD authentication tunnel configuring LDAP server access configuring NIS server access creating an SVM computer account on the domain creating users accounts for providing SVM administrators access defining custom roles enabling Active Directory accounts enabling Active Directory cluster administrator accounts enabling LDAP or NIS user accounts to access SVMs enabling local cluster administrator accounts enabling local user accounts enabling local user accounts to access with an SSH public key generating a digital certificate signing request installing a CA-signed server digital certificate introduction to configuring Active Directory domain controller access introduction to configuring LDAP server access introducing NIS server access managing failed login attempts modifying administrator roles predefined roles for administrators predefined roles for cluster administrators
uninstalling tunnels, AD authentication configuring Twitter how to receive automatic notification of documentation changes unlocking administrator accounts user accounts
Active Directory, enabling for cluster administrators enabling for SVM administrators commands for installing a CA-signed server digital certificate configuring an AD authentication tunnel configuring LDAP server access configuring NIS server access creating an SVM computer account on the domain creating for SVM administrators defining custom roles generating a digital certificate signing request installing a CA-signed server digital certificate introduction to configuring Active Directory domain controller access introduction to configuring LDAP access introducing NIS access local, enabling for cluster administrators local, enabling for SVM administrators managing failed login attempts modifying administrator roles predefined roles for cluster administrators predefined roles for SVM administrators user accounts, local enabling access to SVMs with an SSH public key users, local commands for installing a CA-signed server digital certificate generating a digital certificate signing request installing a CA-signed server digital certificate worksheets to gather configuration information for administrator authentication and RBAC