SnapDrive® 7.1 for Windows®

Installation Guide

February 2019 | 215-08796_D0
doccomments@netapp.com

NetApp®

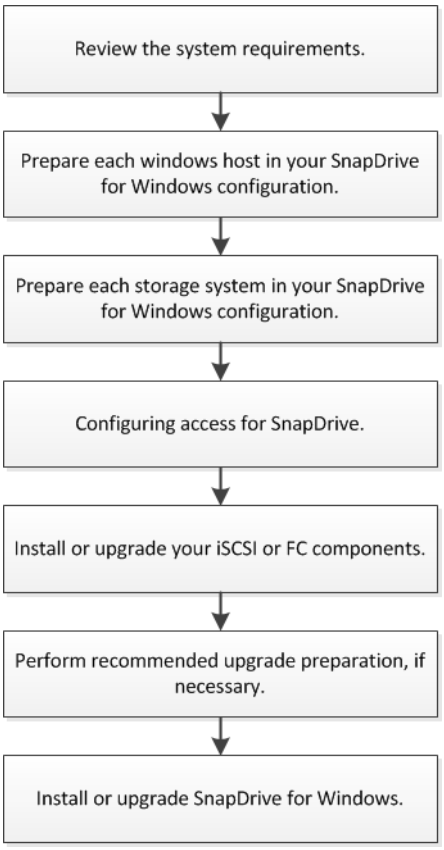
Contents

SnapDrive for Windows installation and setup workflow 5
Understanding SnapDrive for Windows components 6
Understanding SnapDrive licensing 7
SnapDrive licensing 7
Restore, verification, and cloning operation licensing requirements 7
Overview of setting up SnapDrive in clustered Data ONTAP 8
Supported configurations for SnapDrive for Windows 9
Preparing hosts to run SnapDrive for Windows 10
Preparing your Data ONTAP storage systems to run SnapDrive for Windows in 7-Mode environments 11
Configuring access for SnapDrive 12
SnapDrive service account requirements 12
Transport protocol settings support and restrictions 12
Setting up your group Managed Service Account on Windows Server 2012 13
When pass-through authentication might be required 14
Configuring SnapDrive pass-through authentication 15
User account requirements for SnapDrive web services 16
Setting up IPv6 and IPv4 support 16
Installing or upgrading system components that use iSCSI or FC protocols 17
Preparing to upgrade SnapDrive for Windows 18
Installing or upgrading SnapDrive for Windows 19
Remotely installing or uninstalling SnapDrive for Windows from SnapManager for Hyper-V 21
Installing SnapDrive for Windows on Server Core systems 22
Preparing to install SnapDrive for Windows on Windows Server 2008 R2 SP1 and 2012 Server Core and 2016 Server core 22
Enabling remote administration on the Server Core system 22
Renaming the Server Core system 22
Joining the Server Core system to a domain 22
Disabling Windows Server Core firewall 23
Installing .NET Framework on Windows Server 2008 R2 SP1 Server Core and 2012 Server Core 23
Installing .NET Framework on Windows Server 2016 Server Core 23
Installing SnapDrive for Windows on Windows Server 2008 R2 SP1 and 2012 Server Core systems 23
Installing SnapDrive for Windows on a server with no Internet access 25
Unattended SnapDrive installation reference 26
SnapDrive command-line installation syntax 26
SnapDrive upgrade command-line syntax 26

SnapDrive for Windows command-line installation switch descriptions 27
SnapDrive for Windows unattended installation examples 31
Copyright 34
Trademark 35
How to send comments about documentation and receive update notifications 36
Index 37

SnapDrive for Windows installation and setup workflow

The standard SnapDrive for Windows installation workflow includes preparing the Windows hosts, preparing the storage systems, configuring access for SnapDrive for Windows, installing or upgrading FC or iSCSI components, and installing SnapDrive for Windows.



This workflow describes a standard installation or upgrade workflow. This Installation Guide also describes installing SnapDrive for Windows on a Server Core system, performing a remote installation from SnapManager for Hyper-V, installing on systems without Internet access, and installing from a command line. For additional details on installing and setting up SnapDrive for Windows in a clustered Data ONTAP environment, see *SnapDrive for Windows Quick Start Guide for Clustered Data ONTAP*.

Related concepts

Installing SnapDrive for Windows on Server Core systems on page 22

Related tasks

Remotely installing or uninstalling SnapDrive for Windows from SnapManager for Hyper-V on page 21
Installing SnapDrive for Windows on a server with no Internet access on page 25

Related references

Unattended SnapDrive installation reference on page 26

Understanding SnapDrive for Windows components

Several components are integrated into the SnapDrive for Windows software and are automatically installed. These components enable you to manage LUNs, Windows volumes, or SMB shares. You can use these components together to enable SnapDrive for Windows workflows, including provisioning Snapshot copy management; and backup, restore, and mounting operations.

SnapDrive for Windows “snap-in”

This software module integrates with Microsoft Management Console (MMC) to provide you a graphical interface for managing LUNs on the storage system. The module does the following:

- Resides in the Windows Server computer management storage tree
- Provides a native MMC snap-in user interface for configuring and managing LUNs
- Supports remote administration so that you can manage SnapDrive on multiple hosts
- Provides SnapMirror integration
- Provides AutoSupport integration, including event notification

SnapDrive for Windows command-line interface

The `sdcli.exe` utility enables you to manage LUNs from the command prompt of the Windows host. You can perform the following tasks with the `sdcli.exe` utility:

- Enter individual commands
- Run management scripts

PowerShell cmdlets

The SnapDrive for Windows PowerShell cmdlets enable you to perform provisioning; Snapshot copy management; and backup, restore, and mounting operations in an SMB 3.0 environment.

For the latest information about supported PowerShell versions, see the Interoperability Matrix Tool.

NetApp Interoperability Matrix Tool

Underlying SnapDrive for Windows service

This software interacts with software on the storage system to facilitate LUN management for the following:

- A host
- Applications running on a host

ONTAP Volume Shadow Copy Service (VSS) Hardware Provider on Windows Server hosts

The ONTAP VSS Hardware Provider is a module of the Microsoft VSS framework. The ONTAP Hardware Provider enables VSS Snapshot technology on the storage system when SnapDrive for Windows is installed on Windows Server hosts.

Understanding SnapDrive licensing

To optimize SnapDrive for your production environment, you should be aware of the SnapDrive licensing options, and the licensing options associated with some of the tasks you perform.

SnapDrive licensing

Your SnapDrive for Windows license can reside either on the local host or on the storage system that you are using SnapDrive for Windows to manage, depending on how you want to limit or enable operation executions.

- Host-side licensing enables you to execute SnapDrive for Windows operations on any SnapDrive for Windows instance on your host system.
- Storage system licensing enables you to execute SnapDrive for Windows operations only on a storage system that has the SnapDrive for Windows license installed.

In clustered Data ONTAP, you can execute SnapDrive for Windows host-side operations when you have one of the following license configurations:

- Host-side licenses that have a SnapManager license on that host
- A SnapManager_suite license for a clustered Data ONTAP cluster server

In clustered Data ONTAP, you are required to have SnapRestore and FlexClone licenses before setting up your SVM credentials.

Additional licenses you can enable on your storage system

- iSCSI
- Fibre Channel
- SnapRestore® (required for restore operations)
- SnapMirror®
- FlexClone (required for persistent mount operations)
- SnapVault
- MultiStore
- SnapManager suite (if you are using storage system-based licensing)
- NFS
- CIFS (Hyper-V over SMB or SQL Server over SMB workloads)

SnapMirror and SnapVault destinations must have the same feature licenses as your primary storage systems. For example, you require separate SnapManager suite licenses, FlexClone licenses, SnapRestore licenses, and SIS-Clone licenses for each SnapMirror or SnapVault destination storage system.

Restore, verification, and cloning operation licensing requirements

You should be aware of the SnapDrive for Windows licensing requirements for the restore, verification, and cloning operations that you perform with SnapDrive for Windows and the

SnapManager products. The licensing requirements differ based on SAN and SMB 3.0 environments, and whether your systems are operating in 7-Mode or running clustered Data ONTAP.

Task	7-Mode in SAN environments		Clustered Data ONTAP in SAN and SMB 3.0 environments	
	Feature	**License**	**Feature**	**License**
LUN restore from primary	LUN clone split restore	SnapRestore	SIS-Clone	SnapRestore
Restore from secondary SnapVault	Not applicable	N/A	FlexClone	SnapRestore
Hyper-V VSS autorecovery	LUN clone	None	SAN only: SIS-Clone	None
Local verification	LUN clone	None	SAN: FlexClone	FlexClone
	FlexClone	FlexClone	SMB 3.0: FlexClone	FlexClone
Remote verification (SnapMirror and SnapVault)	FlexClone	FlexClone	FlexClone	SnapRestore
DB clone	FlexClone	FlexClone	FlexClone	FlexClone
VM restore, file-level restore, and SMBR	LUN clone	SnapRestore	SIS-Clone	SnapRestore
	FlexClone	SnapRestore and FlexClone	SIS-Clone	SnapRestore

Overview of setting up SnapDrive in clustered Data ONTAP

Setting up and deploying SnapDrive for Windows in clustered Data ONTAP environments requires that you perform several tasks, including setting up your cluster environment, creating an aggregate, virtual storage server, and iSCSI or FC service, configuring your network for the virtual storage server, and creating data volumes.

About this task

For additional information about deploying and configuring SnapDrive for Windows in a clustered Data ONTAP environment, see the *SnapDrive for Windows Quick Start Guide for Clustered Data ONTAP*.

Steps

1. Set up your cluster environment.

   For details, see the *Clustered Data ONTAP Software Setup Guide* for your version of clustered Data ONTAP.

2. Create an aggregate.
3. Create a storage virtual machine (SVM).
4. Set up your SVM credentials.

You do not need to provide cluster credentials; you are required to enter only the SVM credentials. If you have configured your cluster credentials and are running Data ONTAP 8.2 or later, you should remove the cluster credentials.

You must have SnapRestore and FlexClone licenses before setting up your SVM credentials.

If you are configuring and using management LIFs, then the SVMs should use the DNS name of the management LIF, if possible.

5. Create an iSCSI or Fibre Channel (FC) service to set up your iSCSI or FC target node.
6. Configure your network for the SVM with data and management LIFs.
   a. The data LIFs enable the SVM to serve data to the clients (iSCSI or FC.)
   b. The management LIF allows SnapDrive for Windows to communicate with the other LIFs to serve data.
      The management LIF data protocol must be set to “none”.
   c. To connect to the SVM management LIF by using the vsadmin user credentials or equivalent user credentials, you must have HTTP and ONTAPI permissions.
7. Create data volumes for SnapDrive for Windows to create and manage LUNs.
8. For data protection within the cluster, perform the following additional steps:
   a. Create a volume in the virtual storage server of the secondary virtual storage server, and verify that the volume property is of type DP.
   b. Establish a SnapMirror relationship between the primary and the secondary storage systems by accessing the secondary storage system.
9. For intercluster SnapMirror replication, ensure that at least one intercluster management LIF is present in each node on both primary and secondary storage systems.

Supported configurations for SnapDrive for Windows

To install and run SnapDrive for Windows, you must ensure that your storage system and Windows system meet the minimum requirements.

Note: The minimum hardware requirements for installing the Windows Server on the host machine are applicable for SnapDrive for Windows as well.

For the latest information about system requirements and supported storage system versions, see the Interoperability Matrix Tool.

Related information

NetApp Interoperability Matrix Tool

Preparing hosts to run SnapDrive for Windows

Before installing SnapDrive for Windows, you must prepare each Windows host in your SnapDrive for Windows configuration.

Steps

1. Verify that the host meets the minimum requirements for use with SnapDrive for Windows.
2. Determine whether the Microsoft iSCSI Software Initiator program is installed.

   If you are using iSCSI and running Windows Server 2008 or later, the iSCSI Software Initiator comes built in with the operating system, but you must enable it.
3. Determine whether SnapDrive for Windows has been previously installed.
4. Determine which FC or iSCSI HBA or MPIO components are already installed.

Preparing your Data ONTAP storage systems to run SnapDrive for Windows in 7-Mode environments

Before installing SnapDrive for Windows, you must prepare each Data ONTAP storage system operating in 7-Mode in your SnapDrive for Windows configuration.

About this task

Perform the following steps when you are preparing to upgrade your Data ONTAP storage systems operating in 7-Mode.

For information for preparing your clustered Data ONTAP storage systems, see *SnapDrive for Windows Quick Start Guide for Clustered Data ONTAP*.

Steps

1. Verify that the storage system meets the minimum requirements for use with SnapDrive for Windows.
2. After you verify that licenses for FC, iSCSI, or both are enabled on your storage system, you must start the services by entering the `fcp start` command or the `iscsi start` command at the storage system command line.

   See the *Data ONTAP SAN Administration Guide for 7-Mode* for more information.
3. Prepare a volume on the storage system to hold SnapDrive for Windows LUNs.

Configuring access for SnapDrive

Before installing SnapDrive, you must establish a SnapDrive service account and ensure that the authentication requirements are met.

SnapDrive service account requirements

To perform functions related to SnapDrive for Windows on either the host or a storage system, SnapDrive must be able to use a service account that has specific types of access established.

The SnapDrive service account must meet the following requirements:

- The service account must be created using US-ASCII characters only, even when you use non-ASCII operating systems.
- You must be able to log in to the host using the service account.

  Note: If you change the password for this account (for example, from the Windows login panel), you must make the same change to the password that the SnapDrive service uses to log in. You can configure the SnapDrive service using the Services and Applications option in MMC.

- The service account must have administrative rights on the host.

During SnapDrive installation, you are prompted to configure the default transport protocol as RPC, which involves the following further requirements:

- If you are using RPC authentication, the service account must have administrator privileges on both the storage system and the host and must belong to the BUILTIN\Administrators group on the storage system.
- If you are using RPC, the service account must be a domain account, or you can configure pass-through authentication.
- If you are using RPC, the host and storage system must belong to the same domain as the service account or to domains that have direct or indirect trust relationships with the domain to which the service account belongs, or you can configure pass-through authentication.

Transport protocol settings support and restrictions

SnapDrive enables you to use HTTP, HTTPS, and the default RPC protocol for storage system communication. This feature, along with CIFS share dependency removal, enables you to perform SnapDrive-related operations without having root access on the storage system.

SnapDrive enables you to configure HTTP, HTTPS, and RPC for individual storage systems. It also enables you to set a default transport protocol in case one has not been specified for individual storage systems.

You can configure transport protocols either during or after SnapDrive installation.

The `httpd.admin.enable` option must be enabled on the storage system before SnapDrive can use the HTTP or HTTPS protocol.

To improve the performance of SnapDrive system, you must use local admin rights on the storage system instead of using the HTTP protocol in clustered Data ONTAP environments.

The following restrictions apply to transport protocol settings support:

- HTTPS is not supported with MultiStore.
- Using the domain USER account for authentication results in significantly reduced performance. To avoid this issue, you must use a storage system account for authentication instead of the domain account.
- SnapDrive does not support the RPC protocol in a clustered Data ONTAP environment; you must use the HTTP or HTTPS protocol.

Note: If the servers use different protocols, then you must configure SnapDrive to use the same protocol (RPC, HTTP, HTTPS) on all the servers.

Setting up your group Managed Service Account on Windows Server 2012

Windows Server 2012 enables you to create a group Managed Service Account (gMSA) that provides automated service account password management from a managed domain account. Setting up a gMSA eliminates the need for administrators to manually administer passwords for these accounts.

Before you begin

- You have a Windows Server 2012 domain controller.
- You are a Windows Server 2012 domain member with permissions to set up and administer the gMSA.

About this task

You cannot use a gMSA on storage systems configured with RPC protocol settings.

Steps

1. Create a KDS root key to generate unique passwords for each object in your gMSA.

   From the Windows Server 2012 domain controller, run the following command:

   `Add-KDSRootKey -EffectiveImmediately`

   You should complete this step once per domain.

2. Create and configure your gMSA:

   a. Create a user group account with administrator and domain administrator privileges.

   b. Add computer objects to the group.

   c. Use the user group you just created to create the gMSA, as in the following example:

   ```
   New-ADServiceAccount
   -name <ServiceAccountName>
   -DNSHostName <fqdn>
   -PrincipalsAllowedToRetrieveManagedPassword <group>
   -ServicePrincipalNames <SPN1,SPN2,…>
   ```

3. Configure the gMSA on your hosts:

   a. Enable the Active Directory module for Windows PowerShell on the host where you want to use the gMSA account.

To do this, run the following command from PowerShell:

```
PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                            Name                Install
State
------------                            ----
-------------
[ ] Active Directory Domain Services   AD-Domain-Services
Available


PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain
Services, Active ...
WARNING: Windows automatic updating is not enabled. To ensure that
your newly-installed role or feature is
automatically updated, turn on Windows Update.
```

b. Restart your host.

c. Install the gMSA on your host by running the following command from the PowerShell command prompt:

`Install-AdServiceAccount <gMSA>`

d. Test your gMSA account by running the following command:

`Test-AdServiceAccount <gMSA>`

4. Configure SnapDrive with your new gMSA account by installing your SnapDrive service without providing a password.

When pass-through authentication might be required

If you are using RPC authentication, you might need to configure pass-through authentication for SnapDrive between a Windows host and a storage system. You can use HTTP or HTTPS to connect to clustered Data ONTAP systems.

Pass-through authentication might be required in the following situations:

- You do not have a domain controller available.
- You want to install your Windows host as a stand-alone server in a workgroup environment without any dependency on another system for authentication, even if there is a domain controller available.
- Your Windows host and the storage system are in two different domains.
- Your Windows host is in a domain and you want to keep the storage system in a workgroup with no direct access by domain users or the domain controller.

Configuring SnapDrive pass-through authentication

If you are using RPC authentication, you must ensure that pass-through authentication is configured correctly for SnapDrive on both the Windows host and on the storage system.

Before you begin

- You must have root privileges on the storage system.
- You must have administrator privileges on the Windows host.
- If you have a clustered SnapDrive configuration, you must use a domain account to run the cluster service, and all nodes of the cluster must be in the same domain.
  However, the storage system can be in a different domain or workgroup.

Steps

1. Create a user account on the storage system by entering the following command:

   useradmin user add *user_name* -g *group*

   The variables represent the following values:

   - *user_name* is the name of the SnapDrive user.
   - -g is the option you use to specify a user group.
   - *group* is the name of the group to which you want to add the new user.

   #### Example

   The following command adds a user called “snapdrive” to the BUILTIN\Administrators group on the storage system:

   useradmin user add snapdrive -g Administrators

   Note: You must provide this user name later in this procedure. Therefore, make a note of the user name, including the letter case (lowercase or uppercase) of each character in the user name.

2. Enter a password, when prompted to do so, for the user account you are creating.

   You are prompted to enter the password twice. You are required to provide this password later, so make a note of it, including letter case.

3. Check to ensure that the user account you just created belongs to the local administrator's group on the storage system by entering the following command:

   useradmin user list

   For additional information, see the section about creating local groups on the storage system in the *Data ONTAP File Access and Protocols Management Guide for 7-Mode*.

4. On each Windows host that needs access to the storage system, create a local user account with administrative rights on the host, using the same user name and password that you specified in Step 1 and Step 2.

   Note: Set up the local user account so that the password for the account never expires.

   For detailed instructions on how to create local user accounts, see your Windows documentation.

5. If you are using Windows Server 2008, set the SnapDrive service on each host to use the local user account you created in Step 4.

User account requirements for SnapDrive web services

To use SnapDrive via the web services feature, you must log in to a user account that has specific types of access established.

The user account must meet the following requirements.

- If your SnapDrive host is stand-alone, the user account must have administrator privileges on the host or be a member of a group named “SnapDrive Administrators” on the host.
- If your SnapDrive host is part of a Windows domain, the user account can have local or domain administrator privileges, or be a member of a local or domain “SnapDrive Administrators” group.

Setting up IPv6 and IPv4 support

SnapDrive supports IPv6 and IPv4 in clustered Data ONTAP and 7-Mode.

You can provide SnapDrive a host name or IP address in either IPv4 or IPv6 format. Decide which format you are going to use, and then configure it accordingly.

Addresses in IPv6 format are accepted in both expanded and compressed forms. You can use a link-local IPv6 address for iSCSI session management and for communication between a host and a target only when both are in the same subnet.

Installing or upgrading system components that use iSCSI or FC protocols

SnapDrive for Windows supports four protocols for creating and managing LUNs: iSCSI, FC, FCoE, and vFC. Before you install SnapDrive, you must install or upgrade the host system components that use these protocols.

About this task

For the latest software compatibility information, see the Interoperability Matrix.

mysupport.netapp.com/matrix

Step

1. Install or upgrade the required components for the protocols that you plan to use.

If you will create and manage LUNs using...	Then do this...
iSCSI protocol and the software initiator	**a.** Install or upgrade the Microsoft iSCSI Software Initiator. **b.** Install the iSCSI Host Utilities on your hosts. **Note:** If you are running Windows Server 2008, the iSCSI Software Initiator is built into the operating system, but it must be enabled.
iSCSI protocol and the hardware initiator	**a.** Install or upgrade the iSCSI driver and firmware. **b.** Install the iSCSI Host Utilities on your hosts. For a list of supported iSCSI HBAs, see the iSCSI Support Matrix on the NetApp Support Site. For a list of supported HBA drivers or firmware, see the Interoperability Matrix.
FC and Fibre Channel over Ethernet (FCoE) protocol	Install or upgrade the FC driver and firmware. For more information, see the FC Windows Host Utilities for Native OS documentation on the NetApp Support Site. The FC upgrade stops the SnapDrive for Windows service. SnapDrive for Windows restarts when the system is rebooted. If you proceed without a reboot, you must restart the SnapDrive for Windows service manually.
Virtual Fibre Channel (vFC)	**a.** Launch the Hyper-V Manager Virtual SAN Manager wizard. **b.** Follow the instructions to create a new vFC SAN. **c.** Put your VM into the Off state, and select the **Setting** tab for the VM in the Hyper-V Manager Actions pane. **d.** Add up to four Fibre Channel Adapters per VM.

Preparing to upgrade SnapDrive for Windows

If you are upgrading SnapDrive for Windows from an existing installation, you must prepare in a way that is different from preparing to perform a new installation.

Before you begin

Your system must be running one of the following previous versions of SnapDrive for Windows:

- SnapDrive 6.4.2 for Windows
- SnapDrive 6.5 for Windows
- SnapDrive 7.0.x for Windows

Steps

1. Back up your application data.

   If you have SnapManager, use SnapManager rather than SnapDrive for Windows to create a backup copy. Make sure that you have a valid and up-to-date SnapManager backup and that no SnapManager backups are scheduled to occur while you are upgrading. If there are backups scheduled, cancel them.

2. If you are upgrading a server cluster, prepare the hosts by upgrading the operating systems on the cluster nodes to the required Service Pack and hotfix level, if necessary.

   If you must apply a new Service Pack or hotfix, you must also reboot the cluster.

3. Create a full backup, including system state, and create an emergency repair disk for your single system or for each node in a server cluster.

4. If you are upgrading a server cluster, make sure that the cluster groups are online and that you can perform a “move group” operation back and forth between nodes.

   If the cluster service is not running, SnapDrive for Windows cannot collect data necessary for disk enumeration and it causes warning messages to be logged in the Event Viewer.

5. If you are running NetApp Host Agent, stop the NetApp Host Agent service.

   You might have to upgrade NetApp Host Agent, depending on the version you are running. See Interoperability Matrix at *mysupport.netapp.com/matrix* for required versions and compatibility.

6. If you use SnapManager, stop SnapManager before upgrading SnapDrive for Windows.

Installing or upgrading SnapDrive for Windows

After you have completed the installation prerequisites, you should use the Installation wizard to install or upgrade SnapDrive for Windows on your system.

Before you begin

- You must have either a host-side or storage-side SnapDrive for Windows license.
- You must have created a SnapDrive for Windows user account and added it to the local administrators group on your storage system.
- You must have stopped the Windows Host utilities and provisioning and protection capabilities of the OnCommand Unified Manager Core Package.
- You must have installed the appropriate version of PowerShell.
  NetApp Interoperability Matrix Tool

Steps

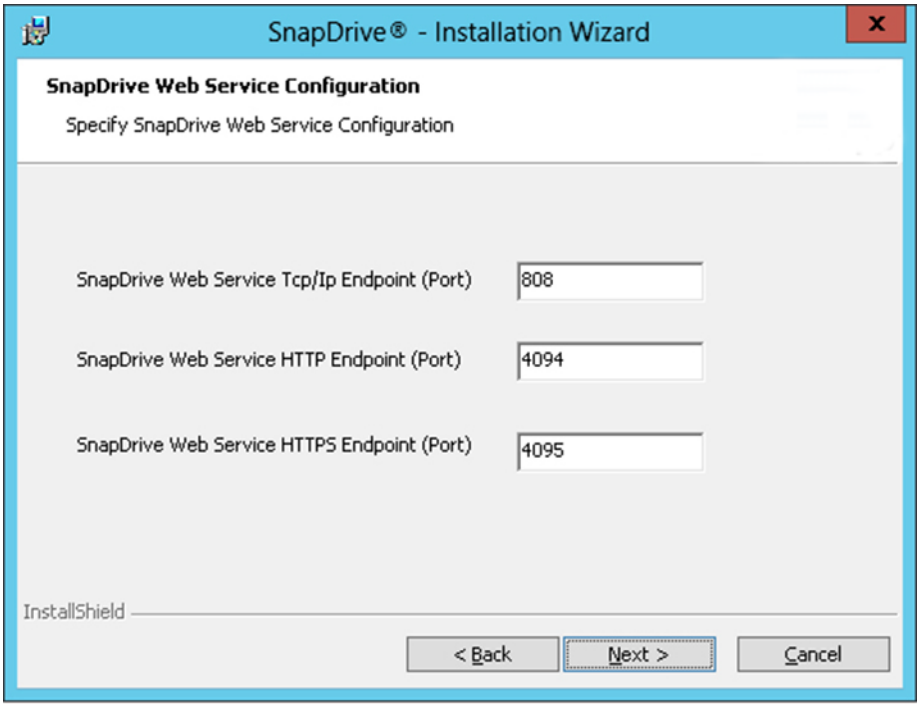
1. Launch the SnapDrive for Windows installer, and then follow the Installation wizard instructions.
2. In the **Firewall** screen, allow SnapDrive for Windows to modify the default Windows firewall rules to enable SnapDrive for Windows to communicate with other SnapDrive for Windows instances.

   If you choose not to allow SnapDrive for Windows to modify the Windows firewall rules, you can either turn Windows firewall off or manually modify the firewall rules later.

   Note: If a firewall is configured on the system, then you can open necessary ports for SnapDrive.

3. In the **SnapDrive Web Service Configuration** screen, accept the default port numbers.

   If you want to change the port numbers, you should also change the port numbers for other SnapDrive hosts.



4. In the **Preferred IP Address** screen, identify the IP address you want to use to communicate with the storage system.

   You should configure the preferred IP address, because doing this improves performance and scalability.

5. In the **Transport Protocol Default Setting** screen, enable the storage protocol settings.

   RPC is not supported in clustered Data ONTAP.

6. If you are working in 7-Mode environments, you can use the **Unified Manager Configuration** screen to provide the information necessary to enable the data protection capabilities of the OnCommand Unified Manager Core Package.

   OnCommand Unified Manager Core Package data protection capabilities are available only in 7-Mode environments.

7. When you have completed the Installation wizard instructions, click **Finish**.

Remotely installing or uninstalling SnapDrive for Windows from SnapManager for Hyper-V

The SnapManager for Hyper-V Remote Host Install wizard enables you to remotely install or uninstall SnapDrive for Windows on standalone and cluster hosts or nodes.

Before you begin

- You must have SnapManager for Hyper-V and SnapDrive for Windows installed on a host node to use the Remote Host Install wizard to remotely install SnapDrive for Windows.
- You must have established a trust relationship between your host node domain and your destination node domain.

Steps

1. From the navigation pane, click **Protection**.
2. From the **Actions** pane, click **Remote Host Install**.
3. Run the **Remote Host Install** wizard.

Result

When you run the Remote Host Install wizard, the host node pushes the SnapDrive for Windows installation or uninstallation to other nodes or hosts in the cluster.

Installing SnapDrive for Windows on Server Core systems

You can install SnapDrive for Windows on Server Core systems after following some preparatory steps. Server Core systems support a minimal Windows Server installation that supports only certain Windows Server roles.

Preparing to install SnapDrive for Windows on Windows Server 2008 R2 SP1 and 2012 Server Core and 2016 Server core

Before you can install SnapDrive for Windows on a Windows Server 2008 R2 SP1, 2012, 2012 R2, or 2016 Server Core system, you must enable remote administration, rename the server, join the domain, and disable the server firewall.

Enabling remote administration on the Server Core system

Before you install SnapDrive for Windows on the Server Core system, you must enable remote administration so you can manage the core SnapDrive instance from a Windows GUI SnapDrive instance.

Steps

1. At the Windows Server Core command prompt, enter the following command:

   netsh advfirewall firewall set rule group="Remote Administration" new enable=yes

2. Enter the following command:

   netsh advfirewall set currentprofile settings remotemanagement enable

Renaming the Server Core system

Before you install SnapDrive for Windows on the Server Core system, you should rename the server to something more meaningful.

Step

1. At the Windows Server Core command prompt, enter the following command:

   netdom renamecomputer *ComputerName* /NewName:*NewComputerName*

Joining the Server Core system to a domain

Before you install SnapDrive for Windows on the Server Core system, you must add the server to the appropriate domain.

Step

1. At the Windows Server Core command prompt, enter the following command:

   netdom join *ComputerName* /domain:*DomainName*/userid:*UserName* / password:*Password*

Disabling Windows Server Core firewall

Before you install SnapDrive for Windows on the Server Core system, you must disable the firewall.

Step

1. At the Windows Server Core prompt, enter the following command:

   `netsh advfirewall set currentprofile state off`

   The `netsh firewall` command is obsolete. Use `netsh advfirewall firewall`.

   For more information, refer to KB article 947709 at the NetApp Support Site at *mysupport.netapp.com*.

Installing .NET Framework on Windows Server 2008 R2 SP1 Server Core and 2012 Server Core

Before you install SnapDrive for Windows on Windows Server 2008 R2 SP1 Server Core and 2012 Server core, you must install the .NET Framework; otherwise, your SnapDrive for Windows installation fails.

Steps

1. Using Deployment Image Servicing and Management (`DISM.exe`), enter the following command at the Microsoft command prompt:

   `Dism /online /enable-feature /featurename:NetFx2-ServerCore`

2. Complete the .NET Framework installation:

   `Dism /online /enable-feature /featurename:NetFx3-ServerCore`

Installing .NET Framework on Windows Server 2016 Server Core

Before you install SnapDrive for Windows on Windows Server 2016 Server Core, you must install the .NET Framework; otherwise, your SnapDrive for Windows installation fails.

Steps

1. Install the .NET Framework 3.5 feature files from Windows Update by entering the following command:

   `Dism /online /enable-feature /featurename:NetFx2-ServerCore`

2. Complete the .NET Framework installation: `DISM /Online /Enable-Feature /FeatureName:NetFx3 /All`

Installing SnapDrive for Windows on Windows Server 2008 R2 SP1 and 2012 Server Core systems

You can install SnapDrive for Windows on Windows Server 2008 R2 SP1, 2012, and 2012 R2 Server Core systems to enable LUN provisioning and Snapshot copy management from a remote instance of SnapDrive for Windows running on a noncore system.

Before you begin

If the LUNs are created and mapped outside SnapDrive, then you must unmap and map the LUNs again using SnapDrive.

The following conditions must exist before you install SnapDrive for Windows on a Server Core system:

- Remote administration must be enabled.
- The Server Core system must be renamed in a meaningful way.
- The Server Core system must be a member of the Windows domain.
- The firewall must be disabled.
- In Windows Server 2008 R2 SP1 Server Core, .NET must be installed, and WCF must be activated.

Steps

1. On a full Windows Server 2008 R2 SP1 or 2012 installation, create a share to the Server Core system using Microsoft Management Console.
2. Download `snapdrive.exe` to a folder on the remote Windows server.
3. Copy `snapdrive.exe` to the share that you created on the remote server.
4. Create a file called `install.bat` on your Server Core system, and then copy the following unattended install command into the file, adding the serial number, password, and user name as necessary:

```
snapdrive7.1.exe
/s /v"/qn SILENT_MODE=1
SERVER_CORE_SYSTEM=1
/Li SDInstall.log
LPSM_SERIALNUMBER=serialnumber
INSTALLDIR=\"c:\Program Files\NetApp\SnapDrive\"
SVCUSERNAME=domain\username
SVCUSERPASSWORD=password
SVCCONFIRMUSERPASSWORD=password
SDW_WEBSRV_TCP_PORT=808
SDW_WEBSRV_HTTP_PORT=4098
ADD_WINDOWS_FIREWALL=1
TRANSPORT_PRT_SELECTION=2
TRANSPORT_PRT_PORT=80
TRANSPORT_PROTOCOL_LOGON_USERNAME=username
TRANSPORT_PROTOCOL_LOGON_PASSWORD=password"
```

   The path `c:\Program Files\NetApp\SnapDrive\` is the default path. You can update this path to any valid directory path. You can also select a path other than the Windows directory path and special directory paths.

5. Either run `install.bat` from the Server Core system command prompt, or enter the unattended install command at the command prompt.

Installing SnapDrive for Windows on a server with no Internet access

When you are installing SnapDrive for Windows on a server with no or limited Internet access, the SnapDrive for Windows service might not start. This is due to the Windows Logo certification requiring a Certificate Revocation list check when the service starts.

Steps

1. Log in to the server as the SnapDrive for Windows service account user.
2. Open Internet Explorer.
3. Go to **Tools > Internet Options > Advanced**.
4. Deselect the “Check for Publisher's certificate revocation” and “Check for server certificate revocation” check boxes.

   Note: These settings are per user and not global, which is why you should be sure to log in as the SnapDrive for Windows service account.

After you finish

If you continue to have problems installing SnapDrive for Windows without Internet access, see the public report for bug ID *757590*.

Unattended SnapDrive installation reference

You can perform unattended SnapDrive installations for first-time installations and for upgrades.

SnapDrive command-line installation syntax

You can run the SnapDrive for Windows installation package from the command-line to perform an unattended installation.

Command syntax

```
snapdrive7.1.exe
/s
[/x]
/v"
/qn
SWITCH1 [SWITCH2 SWITCH3 ...]"
```

/s

Invokes SnapDrive for Windows installation in unattended (also known as *silent*) mode.

/x

Removes SnapDrive for Windows from your system.

/v

When directly followed by `/qn`, enables you to pass arguments and other SnapDrive for Windows installation-specific switches and parameters. These arguments go inside the quotation marks, after the `/qn`.

If you incorrectly enter any of the unattended installation command switches, a pop-up dialog box appears, displaying the correct switch combination or command usage.

SnapDrive upgrade command-line syntax

You can perform a SnapDrive upgrade from the command-line. Command-line upgrades can simplify upgrades on multiple machines.

Command syntax

```
C:\>SnapDrive-7-1-x64.exe /s /v"/qn
REINSTALLMODE=vomus
REINSTALL=ALL SILENT_MODE=1 /Li SDInstall.log
LPSM_SERIALNUMBER=serial number
SVCUSERNAME=domain\username
SVCUSERPASSWORD=password
SVCCONFIRMUSERPASSWORD=password
SDW_WEBSRV_TCP_PORT=808
SDW_WEBSRV_HTTP_PORT=4098
TRANSPORT_PRT_SELECTION=1"
```

SnapDrive for Windows command-line installation switch descriptions

Command-line switches help you customize your unattended SnapDrive for Windows installation.

SILENT_MODE=

Enables SnapDrive for Windows to properly execute the unattended installation feature. This switch is required and you must set it for all unattended installations, including first-time installation, upgrades, and complete uninstallation. Only the following value is valid:

1

Specifies that you would like to perform an unattended installation.

REINSTALLMODE=

Specifies the type of reinstall mode you want to use. The following options are valid values:

v

Indicates that you want to run the installation from the source package and the local package cached. Do not use this option for first-time installations of SnapDrive for Windows.

a

Reinstalls all your SnapDrive for Windows files, regardless of version, date, or checksum value.

o

Reinstalls SnapDrive for Windows files if earlier versions are present or if files are missing.

m

Indicates that you want to rewrite all the SnapDrive for Windows registry entries from HKEY_LOCAL_MACHINE and HKEY_CLASSES_ROOT.

u

Indicates that you want to rewrite all the SnapDrive for Windows registry entries from HKEY_CURRENT_USER and HKEY_USERS.

s

Reinstalls all shortcuts and re-caches all icons, overwriting any existing shortcuts and icons.

REINSTALL=

Specifies that you want to reinstall your SnapDrive for Windows features. The following values are valid:

ALL

Reinstalls all SnapDrive for Windows features.

/Li *filename*

Specifies that you want to generate a SnapDrive for Windows installation log file.

SERVER_CORE_SYSTEM=

Indicates whether you are performing an installation on a Server Core system.

You should use the `SERVER_CORE_SYSTEM=` switch only with Windows Server 2008 Core Server. You should not use the `SERVER_CORE_SYSTEM=` switch with Windows Server 2008 R2 Core Server. The following values are valid:

0

Specifies that you are not installing on a Server Core system.

1

Specifies that you are installing on a Server Core system.

LPSM_SERIALNUMBER=*serialnumber*

Optionally specifies that you want to use the LUN Provisioning and Snapshot Management license for host-side licensing. If you do not provide this license, SnapDrive for Windows looks for a license on the storage system.

INSTALLDIR=*target_directory*

Specifies the target installation directory you want to use for SnapDrive for Windows installations. You only need to use this switch when installing SnapDrive for Windows for the first time.

SVCUSERNAME=*DOMAIN\username*

Specifies the domain and user name you want to use during unattended SnapDrive for Windows installations.

SVCUSERPASSWORD=*password*

Specifies the password you want to use for the `SVCUSERNAME` user. If you have specified your group Managed Service Account (gMSA) as your user name, you do not need to provide a password.

SVCCONFIRMUSERPASSWORD=password

Confirms your `SVCUSERNAME` password.

IGNORE_COMPMGMT_RUNNING=

Indicates whether you want to proceed with the installation, if the MMC is open. The following values are valid:

0

Specifies that you want to abort the SnapDrive for Windows installation if the MMC is open.

1

Specifies that you want the SnapDrive for Windows installation to proceed, even if the MMC is open.

SDW_WEBSRV_TCP_PORT=*port number*

Specifies the port you want SnapDrive for Windows Web services to use for Net.TCP. The default port is 808. This switch is used with new installations only; it is not used for upgrades.

SDW_WEBSRV_HTTP_PORT=*port number*

Specifies which port you want SnapDrive for Windows Web service to use for HTTP. The default port is 4094.

SDW_WEBSRV_HTTPS_PORT=*port number*

Specifies which port you want SnapDrive for Windows Web Service to use for HTTPS. The default port is 4095.

TRANSPORT_SETTING_ENABLE=

Specifies whether you have enabled the transport protocol settings; it is enabled by default. The following values are valid:

0

Indicates that you have disabled the transport protocol settings.

1

Indicates that you have enabled the transport protocol settings.

TRANSPORT_PRT_SELECTION=

Specifies what type of transport protocol you want to use. RPC is the default in a new install or major upgrade. The following values are valid:

1

Indicates that you want to use the RPC transport protocol setting.

2

Indicates that you want to use the HTTP transport protocol setting.

3

Indicates that you want to use the HTTPS transport protocol setting.

TRANSPORT_PRT_PORT=*port number*

Specifies which port you want to use. The default ports are 80 for HTTP and 443 for HTTPS.

TRANSPORT_PROTOCOL_LOGON_USERNAME=*username*

Specifies your user name for HTTP or HTTPS authentication.

TRANSPORT_PROTOCOL_LOGON_PASSWORD=

Specifies your password for HTTP or HTTPS authentication.

DFM_SERVER_INFO=*hostname*

Specifies your OnCommand Unified Manager server name or IP address.

DFM_SERVER_COMM_PRT_SELECTION=

Indicates the type of communication you intend to use for the OnCommand Unified Manager server. The following values are valid:

1

Specifies HTTP as the communication port type.

2

Specifies HTTPS as the communication port type.

DFM_SERVER_COM_PORT=*port*

Specifies your OnCommand Unified Manager server communication port. The default for HTTP is 8088. The default for HTTPS is 8488.

DFM_SERVER_USERNAME=*username*

Specifies the OnCommand Unified Manager server user name you want to use.

DFM_SERVER_PASSWORD=*password*

Specifies your OnCommand Unified Manager server password.

SDW_ESXSVR_ENABLE=

Specifies whether you want to enable the ESX server. The ESX server is disabled by default. The following values are valid:

0

Indicates that you want to disable the ESX server.

1

Indicates that you want to enable the ESX server.

ESXIPADDRESS*IP address*

Specifies the ESX server IP address you want to use.

ESXUSERNAME *username*

Specifies the ESX server user name you want to use.

ESXUSERPASSWORD *password*

Specifies the ESX server password you want to use.

ESXCONFIRMUSERPASSWORD *password*

Confirms the ESX server password you want to use.

SDW_SMVISVR_ENABLE=1

Enables you to add SnapManager for Virtual Infrastructure configuration information.

SMVIIPADDRESS=*IP address name*

Specifies your SnapManager for Virtual Infrastructure server IP address or host name.

SMVIPORT=*SMVIPort*

Specifies the port you want SnapDrive to use to communicate with the SnapManager for Virtual Infrastructure server.

SDW_HYPERV_ENABLE=

Specifies whether Hyper-V pass-through operations are enabled. Disabled is the default. The following values are valid:

0

Indicates that you have disabled Hyper-V pass-through operations.

1

Indicates that you have enabled Hyper-V pass-through operations.

HYPERV_HOSTNAME=*hostname*

Specifies the host name of the current Hyper-V parent host.

HYPERV_IP=*IP address*

Specifies the IP address of the current Hyper-V parent host.

HYPERV_COM_PORT=*port*

Specifies the SnapDrive for Windows Web Service TCP port of the current Hyper-V parent host.

CONFIRM_SDW_UPGRADE

You can use this switch when SnapDrive for Windows is installed with SnapManager products. The following value is valid:

Yes

Specifies that the SnapDrive for Windows upgrade proceeds when SnapManager products are installed.

SKIP_HOTFIX_CHECK

You can use this switch to proceed with the SnapDrive for Windows installation or upgrade when the target system does not yet have all of the required hotfixes installed. Only the following value is valid:

1

Specifies that you want the SnapDrive for Windows upgrade or installation to proceed without the required hotfixes.

ADD_WINDOWS_FIREWALL

You can use this switch to add SnapDrive for Windows to the Windows Firewall. Only the following value is valid:

1

Specifies that you want to include SnapDrive for Windows in the Windows Firewall.

PREFERRED_STORAGE_SYSTEM_NAME=

Specifies the name of the preferred storage system for your SnapDrive for Windows configuration.

PREFERRED_STORAGE_SYSTEM_IP_ADDRESS =

Specifies the IP address for your preferred storage system.

SnapDrive for Windows unattended installation examples

Studying examples that show how to run the SnapDrive for Windows installation package from the command line can help you understand how to perform an unattended installation. Because upgrading from all versions of SnapDrive for Windows is considered a major upgrade, you should follow usage examples carefully.

Complete first time SnapDrive for Windows installation with log

```
SnapDrive7-1x64.exe /s /v"/qn
SILENT_MODE=1
/Li SDinstall.log
LPSM_SERIALNUMBER=serialnumber
INSTALLDIR=\"c:\Program Files\NetApp\SnapDrive\"
SVCUSERNAME=domain\username
SVCUSERPASSWORD=password
SVCCONFIRMUSERPASSWORD=password
SDW_WEBSRV_HTTP_PORT=4098
TRANSPORT_PRT_SELECTION=2
TRANSPORT_PRT_PORT=80
TRANSPORT_PROTOCOL_LOGON_USERNAME=username
TRANSPORT_PROTOCOL_LOGON_PASSWORD=password
ADD_WINDOWS_FIREWALL=1"
```

Complete first time SnapDrive for Windows installation with log, with a Per Server license

```
SnapDrive7-1x64.exe /s /v"/qn
SILENT_MODE=1
/Li SDInstall.log
LPSM_SERIALNUMBER=serialnumber
INSTALLDIR=\"c:\Program Files\NetApp\SnapDrive\"
SVCUSERNAME=domain\username
SVCUSERPASSWORD=password
SVCCONFIRMUSERPASSWORD=password
SDW_WEBSRV_TCP_PORT=808
SDW_WEBSRV_HTTP_PORT=4098
TRANSPORT_PRT_SELECTION=2
TRANSPORT_PRT_PORT=80
TRANSPORT_PROTOCOL_LOGON_USERNAME=username
TRANSPORT_PROTOCOL_LOGON_PASSWORD=password
ADD_WINDOWS_FIREWALL=1"
```

Complete first time SnapDrive for Windows installation with log, with a Per Storage license

```
SnapDrive7-1x64.exe /s /v"/qn
SILENT_MODE=1
/Li SDInstall.log
LPSM_SERIALNUMBER=""
INSTALLDIR=\"c:\Program Files\NetApp\SnapDrive\"
SVCUSERNAME=domain\username
SVCUSERPASSWORD=password
SVCCONFIRMUSERPASSWORD=password
SDW_WEBSRV_TCP_PORT=808
SDW_WEBSRV_HTTP_PORT=4098
TRANSPORT_PRT_SELECTION=2
TRANSPORT_PRT_PORT=80
TRANSPORT_PROTOCOL_LOGON_USERNAME=username
TRANSPORT_PROTOCOL_LOGON_PASSWORD=password
ADD_WINDOWS_FIREWALL=1"
```

Complete first time SnapDrive for Windows installation with log on Windows Server 2008 R2 SP1 Server Core

Do not use this example when you are installing SnapDrive for Windows on Windows Server Core 2008 R2 Server Core.

```
SnapDrive7-1x64.exe /s /v"/qn
SILENT_MODE=1
SERVER_CORE_SYSTEM=1
/Li SDInstall.log
LPSM_SERIALNUMBER=serialnumber
INSTALLDIR=\"c:\Program Files\NetApp\SnapDrive\"
SVCUSERNAME=domain\username
SVCUSERPASSWORD=password
SVCCONFIRMUSERPASSWORD=password
SDW_WEBSRV_TCP_PORT=808
SDW_WEBSRV_HTTP_PORT=4098
TRANSPORT_PRT_SELECTION=2
TRANSPORT_PRT_PORT=80
TRANSPORT_PROTOCOL_LOGON_USERNAME=username
TRANSPORT_PROTOCOL_LOGON_PASSWORD=password
ADD_WINDOWS_FIREWALL=1"
```

Complete first time SnapDrive for Windows installation with log and with ESX server settings disabled

```
SnapDrive7-1x64.exe /s /v"/qn
SILENT_MODE=1
/Li SDInstall.log
LPSM_SERIALNUMBER=serialnumber
INSTALLDIR=\"c:\Program Files\NetApp\SnapDrive\"
SVCUSERNAME=domain\username
SVCUSERPASSWORD=password
SVCCONFIRMUSERPASSWORD=password
SDW_WEBSRV_TCP_PORT=808
SDW_WEBSRV_HTTP_PORT=4098
TRANSPORT_PRT_SELECTION=2
TRANSPORT_PRT_PORT=80
TRANSPORT_PROTOCOL_LOGON_USERNAME=username
TRANSPORT_PROTOCOL_LOGON_PASSWORD=password
```

```
SDW_ESXSVR_ENABLE=0
ADD_WINDOWS_FIREWALL=1"
```

Complete first time SnapDrive for Windows installation with log and with ESX server settings enabled

```
SnapDrive7-1x64.exe /s /v"/qn
SILENT_MODE=1
/Li SDInstall.log
LPSM_SERIALNUMBER=serialnumber
INSTALLDIR=\"c:\Program Files\NetApp\SnapDrive\"
SVCUSERNAME=domain\username
SVCUSERPASSWORD=password
SVCCONFIRMUSERPASSWORD=password
SDW_WEBSRV_TCP_PORT=808
SDW_WEBSRV_HTTP_PORT=4098
TRANSPORT_PRT_SELECTION=2
TRANSPORT_PRT_PORT=80
TRANSPORT_PROTOCOL_LOGON_USERNAME=username
TRANSPORT_PROTOCOL_LOGON_PASSWORD=password
ESXIPADDRESS=IPaddress
ESXUSERNAME=username
ESXUSERPASSWORD=password
ESXCONFIRMUSERPASSWORD=password
ADD_WINDOWS_FIREWALL=1"
```

Upgrade from a previous release

```
SnapDrive7-1x64.exe /s /v"/qn
REINSTALLMODE=vomus
REINSTALL=ALL
SILENT_MODE=1
/Li reSDinstall.log
INSTALLDIR=\"c:\Program Files\NetApp\SnapDrive\"
LPSM_SERIALNUMBER=serialnumber
SVCUSERNAME=domain\username
SVCUSERPASSWORD=password
SVCCONFIRMUSERPASSWORD=password
SDW_WEBSRV_HTTP_PORT=4098
TRANSPORT_PRT_SELECTION=2
TRANSPORT_PRT_PORT=80"
```

Uninstall

```
snapdrive7.1.exe /s /x /v"/qn
SILENT_MODE=1
/Li SDinstall.log"
```

Copyright

Trademark

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

.NET Framework
installing on Windows Server Core *23*

A

access
configuring *12*
pass-through authentication *14*, *15*
aggregates
creating *8*
authentication
HTTP and HTTPS *12*
pass-through *12*, *14*, *15*
RPC *12*

C

cloning operations
licensing requirements for SnapDrive *7*
clustered Data ONTAP
setting up SnapDrive in *8*
command-line installation
examples of SnapDrive unattended *31*
syntax for performing *26*
command-line installations, unattended
switch descriptions for SnapDrive *27*
command-line upgrade
syntax *26*
comments
how to send feedback about documentation *36*
components, SnapDrive for Windows
described *6*
configuration
pass-through authentication *15*
configurations, supported
SnapDrive for Windows *9*
configuring
access *12*
credentials required *12*

D

data volumes
creating *8*
documentation
how to receive automatic notification of changes to *36*
how to send feedback about *36*

E

examples
SnapDrive unattended installation from command line *31*

F

FC protocol
installing *17*
upgrading *17*
feedback
how to send comments about documentation *36*
Fibre Channel service
creating *8*
firewall
disabling before installing SnapDrive for Windows *23*

G

group Managed Service Account
setting up *13*

H

hosts
licensing for *7*
preparing for installation *10*
HTTP and HTTPS
authentication *12*

I

information
how to send feedback about improving documentation *36*
installation
FC components *17*
iSCSI components *17*
SnapDrive on Windows Server Core systems *23*
installation workflow
diagram *5*
installation, command-line
switch descriptions for SnapDrive unattended *27*
installation, remote
from SnapManager for Hyper-V *21*
installation, SnapDrive
unattended *26*
installation, unattended
command-line switch descriptions for SnapDrive *27*
installing
SnapDrive for Windows *5*, *19*
SnapDrive on servers with no Internet access *25*
internet access
installing SnapDrive on servers with no *25*
IPv4 support
in Windows environments *16*
IPv6
support in Windows environments *16*
iSCSI protocol
installing *17*
upgrading *17*
iSCSI service

creating *8*

J

joining Windows Server Core to a domain *22*

L

licenses
for working with SnapDrive *7*
licensing
SnapDrive *7*
licensing requirements
SnapDrive restore, verification, and cloning operation *7*

O

options
licensing, for working with SnapDrive *7*
overview
of installing SnapDrive for Windows *5*

P

pass-through authentication
configuration *15*
reasons to use *14*
password
SnapDrive service account *12*
password management
automated *13*
preparing
for SnapDrive upgrade *18*
preparing for installation
SnapDrive hosts *10*
preparing storage systems
for use with SnapDrive *11*

R

remote administration
enabling on Windows Server Core *22*
remote installation
from SnapManager for Hyper-V *21*
remote uninstallation
from SnapManager for Hyper-V *21*
renaming the Server Core system *22*
requirements
credentials *12*
for SnapDrive service account *12*
SnapDrive restore, verification, and cloning operation licensing *7*
SnapDrive user account *16*
restore operations
licensing requirements for SnapDrive *7*
RPC
authentication *12*

S

service account
establishing to ensure access for SnapDrive *12*
requirements for SnapDrive *12*
service account password management
automating *13*
silent upgrade
syntax *26*
SnapDrive
access configuration *12*
installing pn servers with no Internet access *25*
licensing *7*
licensing requirements for restore, verification, and cloning operations *7*
preparing to install on Windows Server Core *22*
preparing to upgrade *18*
remotely installing from SnapManager for Hyper-V *21*
service account requirements *12*
setting up in clustered Data ONTAP *8*
transport protocol *12*
user account requirements *16*
SnapDrive Administrators group
user account requirements *16*
SnapDrive for Windows
installing on Windows Server Core systems *23*
installing or upgrading *19*
SnapDrive for Windows components
described *6*
SnapDrive for Windows installation
overview *5*
storage system
supported SnapDrive for Windows configurations *9*
storage system communication
enabled by HTTP and HTTPS transport protocol support *12*
storage systems
licensing for *7*
preparing for use with SnapDrive *11*
storage systems operating in 7-Mode
preparing for use with SnapDrive *11*
suggestions
how to send feedback about documentation *36*
supported configurations
SnapDrive for Windows *9*
SVM
creating *8*
switches
description for SnapDrive command-line unattended installation *27*
syntax
command-line upgrade *26*
unattended upgrade *26*
used for an unattended installation *26*
used for command-line installation *26*

T

transport protocols
configuring *12*
default *12*
HTTP and HTTPS support *12*

Twitter
how to receive automatic notification of documentation changes *36*

U

unattended installation
command-line syntax *26*
examples of SnapDrive *31*
of SnapDrive *26*
unattended installations
command-line switch descriptions for SnapDrive *27*
unattended upgrade
syntax *26*
uninstallation, remote
from SnapManager for Hyper-V *21*
upgrades
FC protocol *17*
iSCSI protocol *17*
preparing for SnapDrive *18*
silent *26*
upgrading
SnapDrive for Windows *19*
user access
configuring *12*
user account
requirements *16*

V

verification operations
licensing requirements for SnapDrive *7*
virtual storage servers
configuring your network for *8*

W

Windows Server Core
disabling the firewall before installing SnapDrive for Windows *23*
enabling remote administration *22*
installing .NET Framework on *23*
joining to a domain *22*
preparing to install SnapDrive on *22*
renaming *22*
Windows Server Core systems
installing SnapDrive on *23*
Windows system
supported SnapDrive for Windows configurations *9*
workflow, installation
diagram *5*