IBM System Storage N series

SnapDrive 7.0 for Windows Installation Guide

GC27-5980-00

Contents

Preface

Supported features

IBM System Storage N series storage systems are driven by NetApp Data ONTAP software. Some features described in the product software documentation are neither offered nor supported by IBM. Please contact your local IBM representative or reseller for further details.

Information about supported features can also be found on the N series support website (accessed and navigated as described in *Websites* on page 5).

Websites

IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. The following web pages provide N series information:

- A listing of currently available N series products and features can be found at the following web page:
  www.ibm.com/storage/nas/
- The IBM System Storage N series support website requires users to register in order to obtain access to N series support content on the web. To understand how the N series support web content is organized and navigated, and to access the N series support website, refer to the following publicly accessible web page:
  www.ibm.com/storage/support/nseries/
  This web page also provides links to AutoSupport information as well as other important N series product resources.
- IBM System Storage N series products attach to a variety of servers and operating systems. To determine the latest supported attachments, go to the IBM N series interoperability matrix at the following web page:
  www.ibm.com/systems/storage/network/interophome.html
- For the latest N series hardware product documentation, including planning, installation and setup, and hardware monitoring, service and diagnostics, see the IBM N series Information Center at the following web page:
  publib.boulder.ibm.com/infocenter/nasinfo/nseries/index.jsp

Getting information, help, and service

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you. This section contains

information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your IBM N series product, and whom to call for service, if it is necessary.

Before you call

Before you call, make sure you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure they are connected.
- Check the power switches to make sure the system is turned on.
- Use the troubleshooting information in your system documentation and use the diagnostic tools that come with your system.
- Refer to the N series support website (accessed and navigated as described in *Websites* on page 5) for information on known problems and limitations.

Using the documentation

The latest versions of N series software documentation, including Data ONTAP and other software products, are available on the N series support website (accessed and navigated as described in *Websites* on page 5).

Current N series hardware product documentation is shipped with your hardware product in printed documents or as PDF files on a documentation CD. For the latest N series hardware product documentation PDFs, go to the N series support website.

Hardware documentation, including planning, installation and setup, and hardware monitoring, service, and diagnostics, is also provided in an IBM N series Information Center at the following web page:

publib.boulder.ibm.com/infocenter/nasinfo/nseries/index.jsp

Hardware service and support

You can receive hardware service through IBM Integrated Technology Services. Visit the following web page for support telephone numbers:

www.ibm.com/planetwide/

Firmware updates

IBM N series product firmware is embedded in Data ONTAP. As with all devices, ensure that you run the latest level of firmware. Any firmware updates are posted to the N series support website (accessed and navigated as described in *Websites* on page 5).

Note: If you do not see new firmware updates on the N series support website, you are running the latest level of firmware.

Verify that the latest level of firmware is installed on your machine before contacting IBM for technical support.

How to send your comments

Your feedback helps us to provide the most accurate and high-quality information. If you have comments or suggestions for improving this document, please send them by email to *starpubs@us.ibm.com*.

Be sure to include the following:

- Exact publication title
- Publication form number (for example, GC26-1234-02)
- Page, table, or illustration numbers
- A detailed description of any information that should be changed

Preparing to install or upgrade SnapDrive

Prepare to install or upgrade SnapDrive by familiarizing yourself with an overview of the steps you need to follow to install or upgrade the SnapDrive application software.

Steps

1. Review the system requirements and the N series interoperability matrix website (accessed and navigated as described in *Websites* on page 5) at for the latest information about supported configurations.
2. Prepare each Windows host in your SnapDrive configuration.
3. Prepare each storage system in your SnapDrive configuration.
4. Set up your user credentials for SnapDrive.
5. Install or upgrade the FC or iSCSI components.
6. If you are upgrading an existing SnapDrive installation, perform the recommended upgrade preparations.
7. Install the SnapDrive components.

Understanding your SnapDrive components

Several components are integrated into the SnapDrive 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 workflows, including provisioning, Snapshot copy management, backup, restore, and mounting operations.

The following SnapDrive components are integrated in the software and are automatically installed during installation.

SnapDrive “snap-in”

This software module integrates with Microsoft Management Console (MMC) to provide 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 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 PowerShell cmdlets enable you to perform provisioning, Snapshot copy management and backup, restore, and mounting operations in an SMB 3.0 environment.

SnapDrive supports PowerShell versions 2.0 and later.

Underlying SnapDrive service

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

- A host
- Applications running on a host

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

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

SnapDrive system requirements

You must ensure that your storage system and your Windows system meet at least the minimum requirements to properly install and run SnapDrive.

Note: For the latest system requirements information, see the N series interoperability matrix website (accessed and navigated as described in *Websites* on page 5).

Data ONTAP versions for the storage system

- Data ONTAP 8.0.5 operating in 7-Mode
- Data ONTAP 8.1.3 operating in 7-Mode and clustered environments
- Data ONTAP 8.2.0 operating in 7-Mode and clustered environments

Other system requirements

You should check the N series interoperability matrix website (accessed and navigated as described in *Websites* on page 5) for the latest requirement and interoperability information for related hardware and software:

- Operating systems on the Windows host machine
- Hardware requirements on the Windows host machine or guest VM
- OnCommand Unified Manager Core Package server
- Multipath I/O using Data ONTAP and Microsoft DSM
- IPv4 and IPv6 support
- .NET Framework requirements
- ESX/ESXi server operating system support
- Paravirtual SCSI (PVSCSI adapter support
- Windows hotfixes required for your operating system
- Windows PowerShell 2.0 and later

SnapDrive licensing

Your SnapDrive license can reside either on the local host or on the storage system, that you are using SnapDrive to manage.

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

  In clustered Data ONTAP, you can execute SnapDrive operations with only host-side licenses that have a SnapManager license on a host or the SnapManager_suite license for a clustered Data ONTAP cluster server.

SnapDrive 7.0 for Windows no longer requires that you have cluster credentials. You are only required to set up your virtual storage server credentials. You are required to have a SnapRestore and FlexClone license before setting up your virtual storage server credentials.

Additional licenses you can enable on your storage system

- iSCSI, Fibre Channel, Fibre Channel over Ethernet, or Virtual Fibre Channel
- SnapRestore (required for restore operations)
- SnapMirror
- FlexClone (required for persistent mount operations)
- SnapVault
- MultiStore
- SnapManager products

Preparing hosts for SnapDrive

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

Steps

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

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

Preparing your Data ONTAP storage systems for SnapDrive

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

About this task

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

Steps

1. Verify that the storage system meets the minimum requirements for use with SnapDrive.
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 LUNs.

How volume space is used

SnapDrive uses space on a storage system volume for LUNs and their data, and also for the data that changes between Snapshot copies, the LUN's active file system, and for metadata.

Volume size rules

Storage system volumes that will hold LUNs must be large enough to hold all the LUNs in the volume, as well any Snapshot copies if Snapshot copies are created.

The following factors govern the appropriate minimum size for a volume that holds a LUN:

- If the LUNs are space reserved, then the volume must be more than twice the combined size of all the LUNs on the volume if a Snapshot copy of the volume is created. This enables the volume to hold the LUNs in a fractional reservation area.

  No matter how much the contents of the LUNs change between Snapshot copies, the entire contents of the disks are written to the volume.
- The volume must also provide enough additional space to hold the number of Snapshot copies you intend to keep online.

  The amount of space consumed by a Snapshot copy depends on the amount of data that changes after the Snapshot copy is taken. The maximum number of Snapshot copies is 255 per storage system volume.

Volume and storage system options set by SnapDrive

SnapDrive for Windows automatically checks and resets some storage system and volume options. Key points when SnapDrive checks and resets options:

- When you start SnapDrive
- When you create a LUN
- When you connect a LUN to a host

The following table shows the defaults that are reset and when those resets take place; you should *not* change these values.

Option type	Option	SnapDrive setting	When set
LUN	LUN reserved	LUN reservation set to `Enabled`	• Disk creation
Volume	`nosnapdir`	`Off`	• Disk creation • Disk connection
Volume	Snapshot copy schedule	`Off`	• Disk creation • Disk connection

Volume	`create_ucode`
	`convert_ucode`
	These volume options are no longer used, but they are set to maintain backwards compatibility with earlier versions of SnapDrive.
		`On`	• Disk creation
			• Disk connection

How LUN reservations work

When reservations are enabled for one or more LUNs, Data ONTAP reserves enough space in the volume so that writes to those LUNs do not fail because of a lack of disk space.

Reservations are an attribute of the LUN; they are persistent across storage system reboots, takeovers, and givebacks. Reservations are enabled for new LUNs by default, but you can create a LUN with reservations disabled or enabled.

When a volume contains one or more LUNs with reservations enabled, operations that require free space, such as the creation of Snapshot copies, are prevented from using the reserved space. If these

operations do not have sufficient unreserved free space, they fail. However, writes to the LUNs with reservations enabled continue to succeed.

You can enable reservations for LUNs contained by volumes with volume guarantees of any value. However, if the volume has a guarantee of `none`, reservations do not provide protection against out-of-space errors.

Example

If you create a 100-GB space-reserved LUN in a 500-GB volume, that 100 GB of space is immediately allocated, leaving 400 GB remaining in the volume. In contrast, if space reservation is disabled on the LUN, all 500 GB in the volume remain available until writes are made to the LUN.

Disk space usage with space reservation

When space reservation is enabled, the amount of space available on a volume containing LUNs determines whether Snapshot copy creation can take place.

When you first create a LUN with space reservation enabled, it is granted a space reservation equal to its size. This reserved space is subtracted from the total available disk space on the storage system volume on which the LUN resides.

When you create a Snapshot copy of the storage system volume holding the LUN, that Snapshot copy locks down all the disk blocks occupied by live data.

By monitoring the remaining available space in the storage system volume, the available space in the volume determines whether Snapshot copy creation is allowed. When the amount of available space on the storage system volume falls to below the threshold you set to prevent overwriting space reserved LUNs, Snapshot creation is blocked.

Considerations for setting fractional reserve

Fractional reserve, also called *LUN overwrite reserve*, enables you to control the size of the overwrite reserve for reserved LUNs and files in a volume. By using this volume attribute correctly you can maximize your storage utilization, but you should understand how it interacts with other technologies.

The fractional reserve setting is expressed as a percentage; the only valid values are 0 and 100 percent.

Setting fractional reserve to 0 increases your storage utilization. However, an application accessing data residing in the volume could experience a data outage if the volume is out of free space, even with the volume guarantee set to `volume`, when any of the following technologies and Data ONTAP features is in use:

- Deduplication

- Compression
- FlexClone files
- FlexClone LUNs
- Virtual environments

If you are using one or more of these technologies with no fractional reserve, and you need to prevent errors due to running out of space, you must use all of the following configuration settings for the volume:

- Volume guarantee of `volume`
- File or LUN reservations `enabled`
- Volume Snapshot copy automatic deletion enabled with a commitment level of `destroy`
- Autogrow feature `enabled`

In addition, you must monitor the free space in the associated aggregate. If the aggregate becomes full enough that the volume is prevented from growing, then data modification operations could fail even with all of the other configuration settings in place.

If you do not want to monitor aggregate free space, you can set the volume's fractional reserve setting to 100. This requires more free space up front, but guarantees that data modification operations will succeed even when the technologies listed above are in use.

The default value and allowed values for the fractional reserve setting depend on the guarantee of the volume:

Volume guarantee	Default fractional reserve	Allowed values
Volume	100	0, 100
None	0	0, 100
File	100	100

MultiStore support features and restrictions

If a storage system uses the optional MultiStore feature of Data ONTAP software to create virtual storage system (vFiler units), SnapDrive can create, connect to, and manage LUNs on the vFiler units in the same way it does on the physical storage system.

You accomplish this by providing the name for the vFiler unit rather than the name of the physical storage system to create a connection. It is transparent to the host whether the attached storage system is a physical storage system or a virtual vFiler unit.

If a LUN is in a vFiler unit on storage system with a FlexClone license, SnapDrive attempts to connect to a Snapshot copy using a flexible clone.

Note the following restrictions to MultiStore support:

- SnapDrive is supported on vFiler units only when using the iSCSI protocol.

- The HTTPS protocol is not supported with MultiStore.

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.

Note the following restrictions to transport protocol setting support:

- HTTPS is not supported with MultiStore.
- Using the domain administrator 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 HTTP or HTTPS protocol.

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 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 N series interoperability matrix website (accessed and navigated as described in *Websites* on page 5).

Step

1. Install or upgrade the required components for the protocols 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.** Upgrade or install 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 N series support website (accessed and navigated as described in *Websites* on page 5).
FC and Fibre Channel over Ethernet (FCoE) protocol	Upgrade or install the FC driver and firmware. For more information, see the FC Windows Host Utilities for Native OS documentation on the N series support website (accessed and navigated as described in *Websites* on page 5). The FC upgrade stops the SnapDrive service. SnapDrive restarts when the system is rebooted. If you proceed without a reboot, you must restart the SnapDrive service manually.

If you will create and manage LUNs using...	Then do this...
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 your VM **Setting** tab in the Hyper-V Manager Actions pane. **d.** Add up to four Fibre Channel Adapters per VM.

Preparing to upgrade SnapDrive

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

Before you begin

You must be running SnapDrive 6.4, 6.4.x, or 6.5 to upgrade to SnapDrive 7.0.

Steps

1. Back up your application data.

   If you have SnapManager, use SnapManager rather than SnapDrive 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 is unable to collect data necessary for disk enumeration and causes warning messages to be logged in the Event Viewer.

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

   You might have to upgrade DataFabric Manager Host Agent, depending on the version you are running. See N series interoperability matrix website (accessed and navigated as described in *Websites* on page 5) for required versions and compatibility.

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

Installing or upgrading SnapDrive

After you have prepared by completing the installation prerequisites, you can use the InstallShield wizard to install SnapDrive on your system.

Before you begin

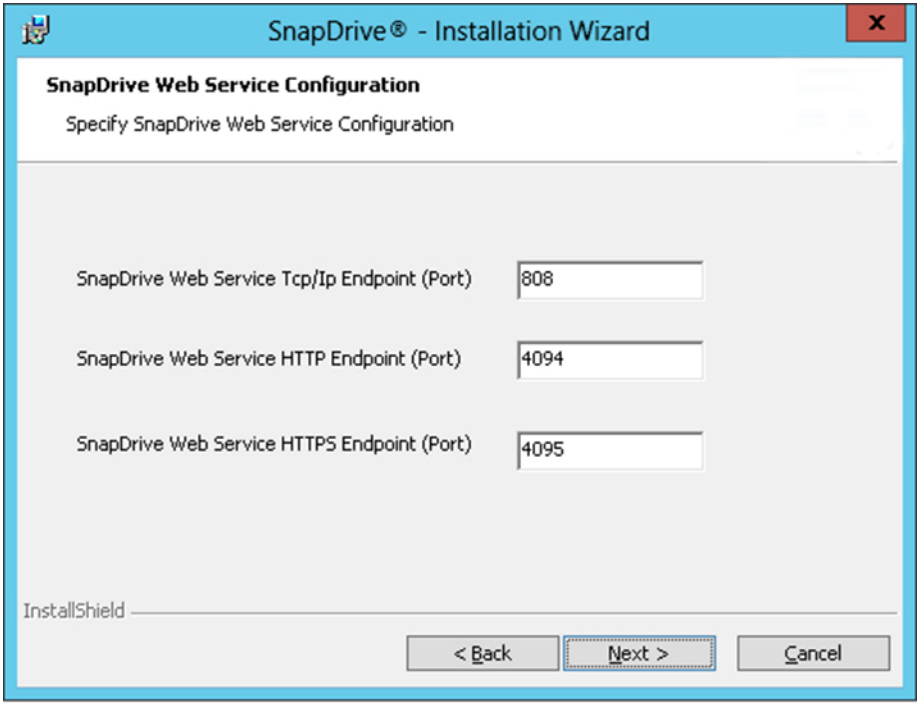
- You have either your host-side or storage-side SnapDrive license.
- You have created your SnapDrive user account and added it to the local administrators group on your storage system.
- You have stopped the Windows Host utilities and provisioning and protection capabilities of the OnCommand Unified Manager Core Package.
- You have PowerShell 2.0 or later installed.

Steps

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

   If you choose not to allow SnapDrive to modify the Windows firewall rules, you can either turn Windows firewall off or manually modify the firewall rules later.
3. In **SnapDrive Web Service Configuration**, you can accept the default port numbers.

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

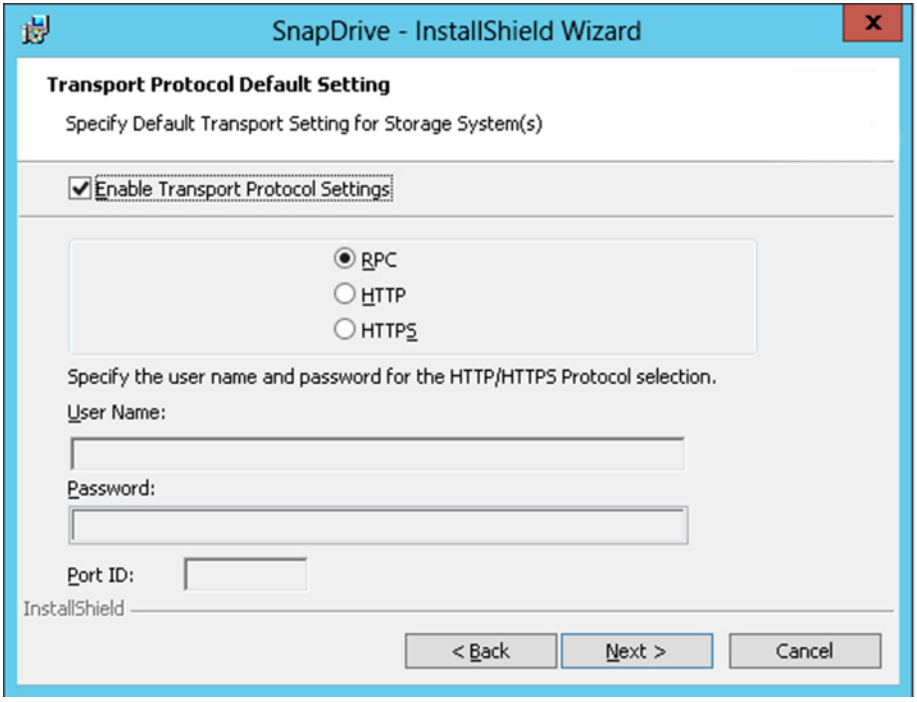


4. In **Preferred IP Address**, you can identify the IP address you want to use to communicate with the storage system.

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

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

   RPC is not supported in clustered Data ONTAP.



6. During **Unified Manager Configuration**, provide the necessary information to enable the data protection capabilities of the OnCommand Unified Manager Core Package.

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

7. When you have completed the InstallShield wizard instructions, click **Finish** to complete your installation.

Remotely installing or uninstalling SnapDrive from SnapManager for Hyper-V

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

Before you begin

- You must have SnapManager for Hyper-V SnapDrive and installed on a host node to use the Remote Host Install wizard to remotely install SnapDrive.
- You 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 installation or uninstallation to other nodes or hosts in the cluster.

Preparing to install SnapDrive on Windows Server 2008 and 2012 Server Core

Before you can install SnapDrive on a Windows Server 2008, 2008 R2, or 2012 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 opmode mode=disable
   ```

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

Installing Microsoft Visual C++ 2008 Redistributable Package on the Server Core system

Before you install SnapDrive for Windows on the Server Core system, you must install Microsoft Visual C++ 2008 Redistributable Package (x64) or your SnapDrive installation will fail.

About this task

This task applies only when you install SnapDrive on Windows Server 2008 Server Core. It does not apply when you install SnapDrive on Windows Server 2008 R2 Server Core.

Steps

1. On a full Windows Server 2008 installation, create a share to the Server Core system using Microsoft Management Console.
2. Download Microsoft Visual C++ 2008 Redistributable Package (x64) from the Microsoft site at www.microsoft.com/downloads/ to a folder on the remote server.
3. Copy the package to the share you created on the remote server.
4. Install the package from the Server Core system command prompt.

Installing .NET Framework on Windows Server 2008 R2 Server Core

Before you install SnapDrive on Windows Server 2008 R2 Server Core, you must install the .NET Framework; otherwise, your SnapDrive 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. To complete the .NET Framework installation, enter the following command:

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

Installing SnapDrive on Windows Server 2008 and 2012 Server Core systems

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

Before you begin

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

- Remote administration is enabled.
- The Server Core system is renamed in a meaningful way.
- The Server Core system is a member of the Windows domain.
- The firewall is disabled.
- In Windows Server 2008 R2, the Microsoft Visual C++ 2008 Redistributable Package (x64) is installed.
- In Windows Server 2008 R2 Server Core, .NET is installed and WCF is activated.

About this task

The `SERVER_CORE_SYSTEM=1` switch must be used only with Windows Server 2008 Server Core installations. Do not use the `SERVER_CORE_SYSTEM=1` switch if you are installing SnapDrive on Windows Server 2008 R2 or Windows Server 2012 Server Core.

Steps

1. On a full Windows Server 2008 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 you created on the remote server.
4. Create a file called `install.bat` on your Server Core system and copy the following unattended install command into the file, adding the serial number, password, and username as necessary:

```
snapdrive7.0.exe /s /v"/qn SILENT_MODE=1 SERVER_CORE_SYSTEM=1 /Li
SDInstall.log LPSM_SERIALNUMBER=serialnumber INSTALLDIR=\"c:\Program
Files\IBM\SnapDrive\" SVCUSERNAME=domain\username
SVCUSERPASSWORD=password SVCCONFIRMUSERPASSWORD=password"
SDW_WEBSRV_TCP_PORT=808 ADD_WINDOWS_FIREWALL=1 SDW_WEBSRV_HTTP_PORT=4098
TRANSPORT_PRT_SELECTION=2 TRANSPORT_PRT_PORT=80
TRANSPORT_PROTOCOL_LOGON_USERNAME=username
TRANSPORT_PROTOCOL_LOGON_PASSWORD=password"
```

The path `c:\Program Files\IBM\SnapDrive\` is the default path. You can update this path to any valid directory path. You can also select a path other than 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 from the command prompt.

Unattended SnapDrive installation reference

You can perform unattended installations of SnapDrive for Windows 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

snapdrive7.0.exe /s [/x] /v"/qn *SWITCH1* [*SWITCH2 SWITCH3* ...]"

/s Invokes SnapDrive installation in unattended (also known as *silent*) mode.

/x Removes SnapDrive from your system.

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

Note: 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-7-0X3-x64.exe /s /v"/qn
REINSTALLMODE=vomus
REINSTALL=ALL SILENT_MODE=1 /Li SDInstall.log
LPSM_SERIALNUMBER=hpbentkyaudcma
SVCUSERNAME=SDSMQA\Administrator
SVCUSERPASSWORD=sdsmqa*123
SVCCONFIRMUSERPASSWORD=sdsmqa*123
SDW_WEBSRV_TCP_PORT=808
SDW_WEBSRV_HTTP_PORT=4098
TRANSPORT_PRT_SELECTION=1"
```

SnapDrive command-line installation switch descriptions

You can use a variety of command-line switches when you perform an unattended installation.

The following table lists, provides values, and describes each of the available command-line installation switches.

Switch	Values and descriptions
`SILENT_MODE=`	**`1`** Enables SnapDrive to properly execute the unattended installation feature. This switch is required and must be set for all unattended installations, including first-time installation, upgrades, and complete uninstallation.
`REINSTALLMODE=`	Specifies the type of reinstall mode to be used: **`v`** Indicates that the installation should be run from the source package and the local package cached. **Note:** Do not use this option for first time installations of SnapDrive. **`a`** Reinstalls all SnapDrive files, regardless of version, date, or checksum value. **`o`** Reinstalls SnapDrive files if earlier versions are present or if files are missing. **`m`** Indicates that all SnapDrive required registry entries FROM HKEY_LOCAL_MACHINE and HKEY_CLASSES_ROOT should be rewritten. **`u`** Indicates that all SnapDrive required registry entries from HKEY_CURRENT_USER and HKEY_USERS should be rewritten. **`s`** Reinstalls all shortcuts and re-caches all icons, overwriting any existing shortcuts and icons.
`REINSTALL=`	**`ALL`** Reinstalls all SnapDrive features.
`/Li`	***`filename`*** Specifies that a SnapDrive installation log should be generated.

Switch	Values and descriptions
SERVER_CORE_SYSTEM=	***0*** Specifies that you are not installing on a Server Core system. ***1*** Specifies that you are installing on a Server Core system. **Note:** You should use the SERVER_CORE_SYSTEM= switch with only Windows Server 2008 Core Server. You should not use the SERVER_CORE_SYSTEM= switch with Windows Server 2008 R2 Core Server.
LPSM_SERIALNUMBER=	***serialnumber*** Optionally specifies the LUN Provisioning and Snapshot Management license for host-side licensing. If you do not provide this license, SnapDrive looks for a license on the storage system operating in 7-Mode. HOST SIDE LICENSE is mandatory for clustered Data ONTAP environments.
INSTALLDIR=	***target installation directory*** Specifies the target installation directory to which SnapDrive will be installed. This switch is required only when installing SnapDrive for the first time.
SVCUSERNAME=	***DOMAIN \username*** Specifies the domain and user name that SnapDrive uses during the unattended installation.
SVCUSERPASSWORD=	***password*** Specifies the password 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 the password for the SVCUSERNAME user.

Switch	Values and descriptions
IGNORE_COMPMGMT_RUNNING=	**0** Specifies that the SnapDrive installation aborts if MMC is open, and a message is displayed indicating that MMC must be closed. **1** Specifies that the SnapDrive installation proceeds, even if MMC is open.
SDW_WEBSRV_TCP_PORT=	***port number*** Specifies which port the SnapDrive Web services should 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 the SnapDrive web service should use for HTTP. The default port is 4094.
SDW_WEBSRV_HTTPS_PORT=	***port number*** Specifies which port the SnapDrive Web Service should use for HTTPS. The default port is 4095.
TRANSPORT_SETTING_ENABLE	Specifies whether the transport protocol settings are enabled. Enabled is the default. **0** Disabled **1** Enabled
TRANSPORT_PRT_SELECTION=	Specifies transport protocol. RPC is the default in a new install or major upgrade. **1** RPC **2** HTTP **3** HTTPS
TRANSPORT_PRT_PORT=	***port number*** Specifies which port should be used. The default ports are 80 for HTTP and 443 for HTTPS.

Switch	Values and descriptions
TRANSPORT_PROTOCOL_LOGON_USERNAME=	***username*** Specifies the user name used for HTTP or HTTPS authentication.
TRANSPORT_PROTOCOL_LOGON_PASSWORD=	***password*** Specifies the password used for HTTP or HTTPS authentication.
DFM_SERVER_INFO=	***hostname*** Specifies the DataFabric Manager server name or IP address.
DFM_SERVER_COMM_PRT_SELECTION=	**1** Specifies HTTP as the communication port type. **2** Specifies HTTPS as the communication port type.
DFM_SERVER_COM_PORT=	***port*** Specifies the DataFabric Manager server communication port. The default for HTTP is 8088. The default for HTTPS is 8488.
DFM_SERVER_USERNAME=	***username*** Specifies the DataFabric Manager server user name.
DFM_SERVER_PASSWORD=	***password*** Specifies the DataFabric Manager server password.
SDW_ESXSVR_ENABLE=	Specifies whether the ESX server is enabled. The ESX server is disabled by default. **0** Disabled **1** Enabled
ESXIPADDRESS	***IP address*** Specifies the ESX server IP address.
ESXUSERNAME	***username*** Specifies the ESX server user name.
ESXUSERPASSWORD	***password*** Specifies the ESX server password.
ESXCONFIRMUSERPASSWORD	***password*** Confirms the ESX server password.

Switch	Values and descriptions
SDW_SMVISVR_ENABLE=	**1** Enables the option to add SMVI configuration information.
SMVIIPADDRESS=	***IP address/ name*** Specifies the SnapManager for Virtual Interface server IP address or host name.
SMVIPORT=	***SMVIPort*** Specifies the port SnapDrive uses 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. **0** Disabled **1** Enabled
HYPERV_HOSTNAME=	***hostname*** Specifies the hostname of the current Hyper-V parent host.
HYPERV_IP=	***IP address*** The IP address of the current Hyper-V parent host.
HYPERV_COM_PORT=	***port*** The SnapDrive Web Service TCP port of the current Hyper-V parent host.
CUSTOMHELP=	**1** Displays usage information for all unattended install switches.
CONFIRM_SDW_UPGRADE	You can use this switch when SnapDrive is installed with SnapManager products. **Yes** Specifies that the SnapDrive upgrade proceeds when SnapManager products are installed.

Switch	Values and descriptions
SKIP_HOTFIX_CHECK	You can use this switch to proceed with the SnapDrive installation or upgrade when the target system does not yet have all of the required hotfixes installed. **1** Specifies that the SnapDrive upgrade or installation should proceed without the required hotfixes.
ADD_WINDOWS_FIREWALL	You can use this switch to add SnapDrive to the Windows Firewall. **1** Specifies that you want to include SnapDrive in the Windows Firewall.

SnapDrive unattended installation examples

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

Examples of commands used to perform unattended SnapDrive installations

The example provided for a complete first time SnapDrive installation on Windows Server 2008 Server Core should not be used when installing SnapDrive on Windows Server Core 2008 R2 Server Core.

Custom help:	**snapdrive7.0.exe /s /v"/qn CUSTOMHELP=1"**
Uninstall:	**snapdrive7.0.exe /s /x /v"/qn SILENT_MODE=1 /Li *SDinstall.log*"**
Complete first time SnapDrive installation with log	**snapdrive7.0.exe /s /v"/qn SILENT_MODE=1 /Li *SDInstall.log* LPSM_SERIALNUMBER=*serialnumber* INSTALLDIR=\"c:\Program Files\IBM\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 installation with log, with a Per Server license

```
snapdrive7.0.exe /s /v"/qn SILENT_MODE=1 /Li SDInstall.log
LPSM_SERIALNUMBER=serialnumber INSTALLDIR=\"c:\Program
Files\IBM\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 LPSM_SERIALNUMBER=serialnumber
```

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

```
snapdrive7.0.exe /s /v"/qn SILENT_MODE=1 /Li SDInstall.log
LPSM_SERIALNUMBER="" INSTALLDIR=\"c:\Program Files\IBM
\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 installation with log on Windows Server 2008 Server Core

```
snapdrive7.0.exe /s /v"/qn SILENT_MODE=1
SERVER_CORE_SYSTEM=1 /Li SDInstall.log
LPSM_SERIALNUMBER=serialnumber INSTALLDIR=\"c:\Program
Files\IBM\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
```

VMware-specific examples

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

```
snapdrive7.0.exe /s /v"/qn SILENT_MODE=1 /Li
SDInstall.log LPSM_SERIALNUMBER=serialnumber INSTALLDIR=
\"c:\Program Files\IBM\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 installation with log and with ESX server settings enabled:	**snapdrive7.0.exe /s /v"/qn SILENT_MODE=1 /Li *SDInstall.log* LPSM_SERIALNUMBER=*serialnumber* INSTALLDIR= \"c:\Program Files\IBM\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**

Overview of setting up SnapDrive in clustered Data ONTAP

Setting up and deploying SnapDrive 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.

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 virtual storage server.
4. Create an iSCSI or Fibre Channel (FC) service to set up your iSCSI or FC target node.
5. Configure your network for the virtual storage server with data and management LIFs.
   a. The data LIFs, which enable virtual storage servers to serve data to the clients (iSCSI or FC.)
   b. The management LIF, which allows SnapDrive to communicate with the other LIFs to serve data. Ensure that the management LIF data protocol is set to "none."
6. Create data volumes for SnapDrive to use to create and manage LUNs.
7. 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 ensure that the volume property is type DP.
   b. Establish a SnapMirror relationship between the primary and the secondary storage systems by accessing the secondary storage system.
8. For intercluster SnapMirror replication, make sure that at least one intercluster management LIF is present in each node on both primary and secondary storage systems.

Copyright and trademark information

References in this documentation to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's or NetApp's intellectual property rights may be used instead of the IBM or NetApp product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM and NetApp, are the user's responsibility.

No part of this document covered by copyright may be reproduced in any form or by any means— graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT

(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S.A. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark information

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. A complete and current list of other IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

NetApp, the NetApp logo, Network Appliance, the Network Appliance logo, Akorri, ApplianceWatch, ASUP, AutoSupport, BalancePoint, BalancePoint Predictor, Bycast, Campaign Express, ComplianceClock, Cryptainer, CryptoShred, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, DenseStak, Engenio, Engenio logo, E-Stack, FAServer, FastStak, FilerView, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Manage ONTAP, MetroCluster, MultiStore, NearStore, NetCache, NOW (NetApp on the Web), Onaro, OnCommand, ONTAPI, OpenKey, PerformanceStak, RAID-DP, ReplicatorX, SANscreen, SANshare, SANtricity, SecureAdmin, SecureShare, Select, Service

Builder, Shadow Tape, Simplicity, Simulate ONTAP, SnapCopy, SnapDirector, SnapDrive, SnapFilter, SnapLock, SnapManager, SnapMigrator, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapSuite, SnapValidator, SnapVault, StorageGRID, StoreVault, the StoreVault logo, SyncMirror, Tech OnTap, The evolution of storage, Topio, vFiler, VFM, Virtual File Manager, VPolicy, WAFL, Web Filer, and XBB are trademarks or registered trademarks of NetApp, Inc. in the United States, other countries, or both.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

NetApp, Inc. is a licensee of the CompactFlash and CF Logo trademarks.

NetApp, Inc. NetCache is certified RealSystem compatible.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe on any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, N.Y. 10504-1785
U.S.A.

For additional information, visit the web at:
http://www.ibm.com/ibm/licensing/contact/

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM web sites are provided for convenience only and do not in any manner serve as an endorsement of those web sites. The materials at those web sites are not part of the materials for this IBM product and use of those web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

Index

T

U

V

W

NA 210-06160_A0, Printed in USA

GC27-5980-00