



NetApp Data Broker 1.0

Deployment Guide
for SnapCenter Plug-in for VMware vSphere

July 2019 | 215-14880_A0
doccomments@netapp.com

Contents

DECIDING WHETHER TO READ THE DEPLOYMENT GUIDE FOR SNAPCENTER PLUG-IN FOR VMWARE VSPHERE.....	4
OVERVIEW OF THE NETAPP DATA BROKER VIRTUAL APPLIANCE FOR SNAPCENTER PLUG-IN FOR VMWARE VSPHERE	5
GETTING STARTED WORKFLOWS.....	7
SnapCenter deployment for new users	7
SnapCenter deployment for existing users	7
ADDING SNAPCENTER LICENSES	9
SnapCenter Standard controller-based licenses	9
SnapCenter Standard capacity-based licenses.....	9
DEPLOYING THE VIRTUAL APPLIANCE FOR SNAPCENTER PLUG-IN FOR VMWARE VSPHERE.....	11
Deployment planning and requirements	11
Host requirements	11
Software support.....	12
Space and sizing requirements	12
Connection and port requirements	13
Configurations supported	13
RBAC privileges required.....	13
AutoSupport.....	14
Downloading the NetApp Data Broker OVA (Open Virtual Appliance).....	14
Deploying the NetApp Data Broker virtual appliance.....	14
Creating a virtual appliance credential for migrating backups.....	17
Registering the SnapCenter Plug-in for VMware vSphere with SnapCenter Server	17
LOGGING IN TO THE SNAPCENTER VMWARE VSPHERE WEB CLIENT	19
WHEN TO USE THE SNAPCENTER GUI AND THE SNAPCENTER VSPHERE WEB CLIENT.....	20
MANAGING THE NETAPP DATA BROKER VIRTUAL APPLIANCE	21
Modifying the time zone for backups.....	21
Modifying the NetApp Data Broker logon credentials.....	21
Modifying the vCenter logon credentials in the NetApp Data Broker	22
MIGRATING TO THE VIRTUAL APPLIANCE FOR SNAPCENTER PLUG-IN FOR VMWARE VSPHERE.....	23
Migrating from SnapCenter to the virtual appliance for SnapCenter Plug-in for VMware vSphere	23
ACCESSING THE MAINTENANCE CONSOLE	26
DISABLING THE SNAPCENTER PLUG-IN FOR VMWARE VSPHERE.....	27
REMOVING THE SNAPCENTER PLUG-IN FOR VMWARE VSPHERE.....	28
TROUBLESHOOTING	29
vCenter MOB entry for the SnapCenter plug-in is not updated	29
VMware vSphere web client GUI not working correctly	29
Restarting the vSphere web client service in Linux.....	29
Restarting the vSphere web client service in Windows	30
Authentication error	31
Bad gateway error.....	31
Cannot download job logs	32
Cannot unmount a backup.....	32
You may have reached the maximum number of NFS volumes configured in the vCenter	32
Unable to discover datastores on an SVM without a management LIF	32
Plug-in is still listed in vCenter after being removed	33
“Bad Gateway” error during migration	33
Information not displayed after upgrading to a new patch of the same release	33
Resources not available if NetApp Data Broker is stopped in linked vCenter	34
COPYRIGHT INFORMATION.....	36
TRADEMARK INFORMATION	37

HOW TO SEND YOUR COMMENTS ABOUT DOCUMENTATION AND RECEIVE UPDATE NOTIFICATIONS..... 38

Deciding whether to read the Deployment Guide for SnapCenter Plug-in for VMware vSphere

This information describes how to deploy and remove the Linux-based NetApp Data Broker virtual appliance (Open Virtual Appliance format) which enables the SnapCenter Plug-in for VMware vSphere. It also describes how to register the plug-in with SnapCenter Server to support application-consistent backup and restore operations.

Overview of the NetApp Data Broker virtual appliance for SnapCenter Plug-in for VMware vSphere

For SnapCenter 4.2 and later, the SnapCenter Plug-in for VMware vSphere is deployed in the NetApp Data Broker Linux-based virtual appliance.

When the SnapCenter Plug-in for VMware vSphere feature is enabled in NetApp Data Broker, the virtual appliance adds the following functionality to your environment:

- Support for VM-consistent and crash-consistent data protection operations for VMware virtual machines (VMs) and datastores.
- Support for SnapCenter application-consistent (application over VMDK/RDM) data protection operations for databases and file systems on primary and secondary storage on VMs.

The SnapCenter Plug-in for VMware vSphere features provided by the virtual appliance include the following:

- Support for VMs, VMDKs, and datastores
The plug-in provides a VMware vSphere web client in vCenter. You use the web client GUI to perform VM-consistent backups of VMs, VMDKs, and datastores. You can also restore VMs and VMDKs, and restore files and folders that reside on a guest OS.

Note: When backing up VMs, VMDKs, and datastores, the plug-in does not support RDMs. Backup jobs for VMs ignore RDMs. If you need to back up RDMs, you must use a SnapCenter application-based plug-in.

The plug-in also provides a MySQL database on the virtual appliance VM that contains SnapCenter Plug-in for VMware vSphere metadata.

- Support for virtualized databases
The plug-in supports backup, recovery, and cloning of virtualized applications and file systems (for example, virtualized SQL, Oracle, and Exchange databases) when you have the appropriate application-based SnapCenter plug-ins installed and you are using SnapCenter to perform data protection operations. Data protection operations are managed using the SnapCenter GUI. SnapCenter natively leverages the SnapCenter Plug-in for VMware vSphere for all data protection operations on VMDKs, raw device mappings (RDMs), and NFS datastores. After the virtual appliance is deployed, the plug-in handles all interactions with vCenter. The plug-in supports all SnapCenter application-based plug-ins.

Note: SnapCenter does not support single Snapshot copies of databases and VMs together. Backups for VMs and databases must be scheduled and run independently, which creates separate Snapshot copies, even if the databases and VMs are hosted in the same volume. Database application backups must be scheduled by using the SnapCenter GUI; VM and datastore backups must be scheduled by using the SnapCenter vSphere web client GUI.

- VMware Tools is required for VM consistent Snapshot copies
If VMware Tools is not installed and running, the file system is not quiesced and a crash-consistent Snapshot is created.
- VMware vMotion is required for restore operations in SAN (VMFS) environments
The restore workflow for VMware file system (VMFS) utilizes the VMware Storage vMotion feature. Storage vMotion is a part of the vSphere Standard License but is not available with the vSphere Essentials or Essentials Plus licenses.

Most restore operations in NFS environments use native ONTAP functionality (for example, Single File SnapRestore) and do not require VMware Storage vMotion.

- The virtual appliance is deployed as a Linux VM
Although the virtual appliance must be installed as a Linux VM, the SnapCenter Plug-in for VMware vSphere supports both Windows-based and Linux-based vCenters. SnapCenter natively uses this plug-in without user intervention to communicate with your vCenter to support SnapCenter application-based plug-ins that perform data protection operations on Windows and Linux virtualized applications.
- Backup jobs for VMs and datastores must be migrated to the SnapCenter Plug-in for VMware vSphere
 - Backup jobs performed by SnapCenter Plug-in for VMware vSphere 4.0, 4.1, and 4.1.1 must be migrated to SnapCenter Plug-in for VMware vSphere 4.2. You migrate these backups by using Windows PowerShell cmdlets in SnapCenter 4.2.
 - Backup jobs performed by VSC with SnapManager for Virtual Infrastructure (SMVI) can be migrated to SnapCenter Plug-in for VMware vSphere 4.2. You migrate these backups by using the *NetApp Import Utility for SnapCenter and Virtual Storage Console*, which is in the NetApp Support Toolchest.

[NetApp Import Utility for SnapCenter and Virtual Storage Console](#)

In addition to these major features, the SnapCenter Plug-in for VMware vSphere also provides support for iSCSI, Fibre Channel, FCoE, VMDK over NFS 3.0 and 4.1, and VMDK over VMFS 5.0 and 6.0.

For the latest information about supported versions, see the [NetApp Interoperability Matrix Tool \(IMT\)](#).

For information about NFS protocols and ESXi, see the VMware "vSphere Storage" documentation.

For information about SnapCenter data protection, see the Data Protection Guide for your SnapCenter plug-in in the [SnapCenter Documentation Center](#).

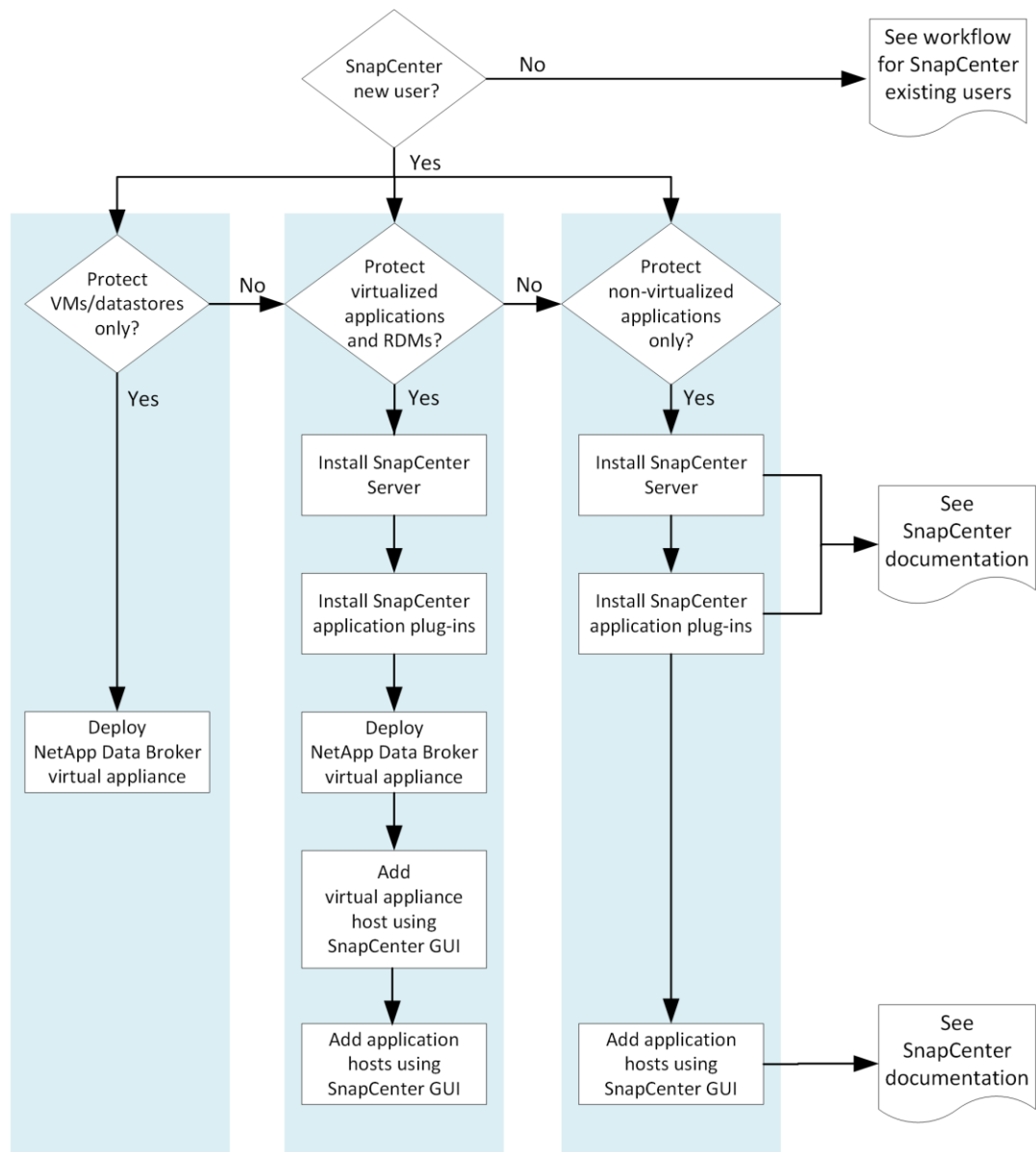
For information about data protection using the SnapCenter Plug-in for VMware vSphere, see the [NetApp Data Broker Data for Guide for SnapCenter Plug-in for VMware vSphere](#).

Getting started workflows

Existing SnapCenter users must use a different deployment workflow from new SnapCenter users.

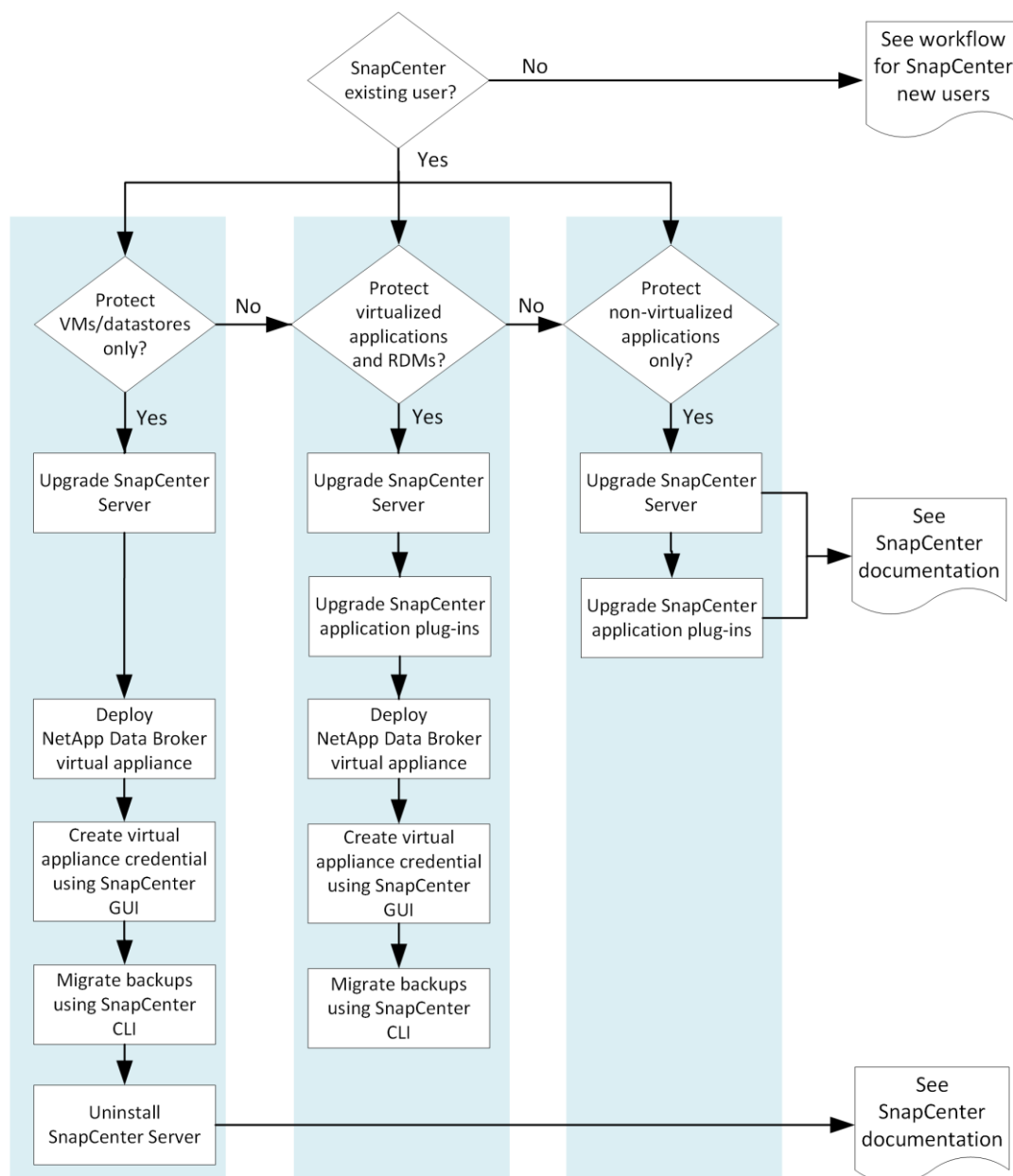
SnapCenter deployment for new users

If you have not used SnapCenter before and do not have any SnapCenter backups, then use this workflow to get started.



SnapCenter deployment for existing users

If you are a SnapCenter user and have SnapCenter backups, then use this workflow to get started.



Adding SnapCenter licenses

The SnapCenter Standard license enables the protection of applications, databases, files systems, and virtual machines. Before you add a storage system to the SnapCenter Plug-in for VMware vSphere, you must install one or more SnapCenter licenses.

The type of SnapCenter licenses you install depends on your storage environment and the features that you want to use.

To enable protection of applications, databases, file systems, and virtual machines, you must have either a Standard controller-based license installed on your FAS or AFF storage system, or a Standard capacity-based license installed on your ONTAP Select and Cloud Volumes ONTAP platforms.

A SnapCenter Standard controller-based or Standard capacity license enables you add an SVM (storage virtual machine) to a SnapCenter instance to provide support for all data protection operations provided by SnapCenter plug-ins on ONTAP storage.

Best Practice: It is recommended, but not required, that you also add SnapCenter Standard licenses to secondary destinations. If SnapCenter Standard licenses are not enabled on secondary systems, you cannot use SnapCenter after performing a failover operation. However, FlexClone license on secondary is required to perform clone and verification operations.

You can view information about your currently installed capacity-based licenses on the SnapCenter Dashboard.

SnapManager Suite licenses apply only to FAS and All Flash FAS SVMs on primary storage systems.

SnapCenter Standard controller-based licenses

A SnapCenter Standard controller-based license is required if you are using FAS or AFF storage controllers.

The controller-based license has the following characteristics:

- SnapCenter Standard entitlement included with purchase of Premium or Flash Bundle (not with the base pack)
- Unlimited storage usage
- Enabled by adding it directly to the FAS or AFF storage controller by using either the OnCommand System Manager or the storage cluster command line

Note: You do not enter any license information in the SnapCenter GUI for the SnapCenter controller-based licenses.

- Is locked to the controller's serial number

Note: If you already have a SnapManagerSuite license on your controller, SnapCenter Standard controller-based license entitlement is provided automatically. The names SnapManagerSuite license and SnapCenter Standard controller-based license are used interchangeably, but they refer to the same license.

For information on viewing, retrieving, and adding controller-based licenses, see the [SnapCenter Installation and Setup Guide](#).

SnapCenter Standard capacity-based licenses

You use a SnapCenter Standard capacity license to protect data on ONTAP Select and Cloud Volumes ONTAP platforms.

The capacity-based license has the following characteristics:

- Composed of a nine-digit serial number with the format 51xxxxxxx
You use the license serial number and valid NetApp Support Site login credentials to enable the license using the SnapCenter GUI.
- Available as a separate, perpetual license, with the cost based on either the used storage capacity or the size of the data you want protected, whichever is lower, and the data is managed by SnapCenter
- Available per terabyte
For example, you can obtain a capacity-based license for 1 TB, 2 TBs, 4 TBs, and so on.
- Available as a 90-day trial license with 100 TB capacity entitlement

For information on retrieving and adding capacity-based licenses, see the [SnapCenter Installation and Setup Guide](#).

Deploying the virtual appliance for SnapCenter Plug-in for VMware vSphere

For SnapCenter 4.2 and later, the SnapCenter Plug-in for VMware vSphere is deployed as part of the Linux-based NetApp Data Broker virtual appliance.

Deployment planning and requirements

You should be aware of the deployment requirements before you deploy the NetApp Data Broker virtual appliance for SnapCenter Plug-in for VMware vSphere.

Host requirements

Before you begin deployment of the NetApp Data Broker virtual appliance for SnapCenter Plug-in for VMware vSphere, you should be familiar with the host requirements.

- You must deploy the NetApp Data Broker virtual appliance as a Linux VM.
The NetApp Data Broker virtual appliance is deployed as a Linux VM regardless of whether you use the plug-in to protect data on Windows systems or Linux systems.
- You should deploy the virtual appliance on the vCenter Server.
Backup schedules are executed in the time zone in which the virtual appliance is deployed. vCenter reports data in the time zone in which the vCenter is located. Therefore, if the virtual appliance and the vCenter are in different time zones, data in the SnapCenter Plug-in for VMware vSphere Dashboard might not be the same as the data in the reports.
- You must not deploy the virtual appliance in a folder that has a name with special characters.
The folder name should not contain the following special characters:
\$! @ # % ^ & () _ + { } ' ; , * ? " < > |
- You must deploy and register a separate, unique instance of the virtual appliance for each vCenter Server.
 - Each vCenter Server, whether or not it is in Linked Mode, must be paired with a separate instance of the virtual appliance.
 - Each instance of the virtual appliance must be installed as a separate Linux VM.
For example, if you want to perform backups from six different instances of the vCenter Server, then you must deploy the virtual appliance on six hosts and each vCenter Server must be paired with a unique instance of the virtual appliance.
- The SnapCenter Plug-in for VMware vSphere provides limited support of shared PCI or PCIe devices (for example, NVIDIA Grid GPU) due to a limitation of the virtual machines in supporting Storage vMotion. For more information, see the vendor's document *Deployment Guide for VMware*.
 - What is supported:
 - Creating resource groups
 - Creating backups without VM consistency
 - Restoring a complete VM when all the VMDKs are on a NFS datastore and the plug-in does not need to use Storage vMotion
 - Attaching and detaching VMDKs
 - Mounting and unmounting datastores
 - Guest file restores
 - What is not supported:
 - Creating backups with VM consistency

- Restoring a complete VM when one or more VMDKs are on a VMFS datastore.
- The SnapCenter Plug-in for VMware vSphere does not support the following:
 - VMware vSphere Thick Clients. You must use the web client.
 - Windows dynamic disks
 - VMware RUC tool
 - NFS 4.1 configured with Kerberos authentication on ESXi and storage
 - pNFS
 - VSAN or VVOL datastores (SAN and NAS datastores are supported)
 - RDM data. The plug-in does not support RDMs for VM backups. If a VM contains RDM LUNs, those LUNs are skipped during backups. To back up RDM LUNs, you must use a SnapCenter application-based plug-in.
 - Datastores that contain only ISO files. To back up datastores that contain only ISO files, you must create a dummy VM in the datastore and then back up that VM.
 - Virtual machine entities like Independent Persistent Disks or .VSWP files that reside on non-NetApp datastores.

Software support

Item	Supported versions
SnapCenter Plug-in for VMware vCenter	NetApp Data Broker 1.0 or later SnapCenter 4.2 or later
VMware vSphere	6.5 or later
vCenter	Flex client: 6.0U3, 6.5U2/U3, 6.7, 6.7U1 HTML5 client: 6.5U2d/U3, 6.7, 6.7U1
ESXi	5.5, 6.0 or later
IP addresses	IPv4 IPv6 is not supported
Java	8
.Net Core	2.1
NetApp Data Broker repository	MySQL 8.0.16
VMware TLS	1.2
TLS on the SnapCenter Server	TLSv1.1 and later The SnapCenter Server uses this to communicate with the virtual appliance for application over VMDK data protection operations.

For the latest information about supported versions, see the [NetApp Interoperability Matrix Tool \(IMT\)](#).

Space and sizing requirements

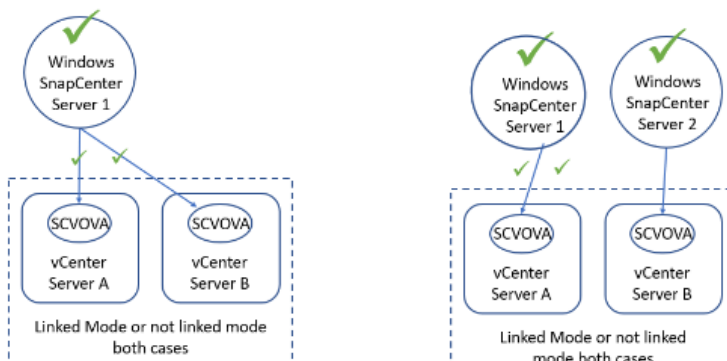
Item	Requirements
Operating system	Linux
Minimum CPU count	4 cores
Minimum RAM	Minimum: 12 GB Recommended: 16 GB
Minimum hard drive space for the SnapCenter Plug-in for VMware vSphere, logs, and repository	100 GB

Connection and port requirements

Type of port	Preconfigured port
SnapCenter Plug-in for VMware vSphere port	<p>8144 (HTTPS), bidirectional The port is used for communications from the vCenter vSphere web client and from the SnapCenter Server.</p> <p>8080 bidirectional This port is used to manage the virtual appliance.</p> <p>Note: You cannot modify the port configuration.</p>
VMware vSphere vCenter Server port	<p>443 (HTTPS), bidirectional The port is used for communication between the SVM host for the SnapCenter Plug-in for VMware vSphere and vCenter.</p>

Configurations supported

Each plug-in instance supports only one vCenter Server. vCenters in linked mode are supported. Multiple plug-in instances can support the same SnapCenter Server.



RBAC privileges required

The vCenter administrator account must have the required vCenter privileges.

To do this operation...	You must have these vCenter privileges...
Deploy and register the SnapCenter Plug-in for VMware vSphere in vCenter	Extension: Register extension
Upgrade or remove the SnapCenter Plug-in for VMware vSphere	Extension <ul style="list-style-type: none"> • Update extension • Unregister extension
Allow the vCenter Credential user account registered in SnapCenter to validate user access to the SnapCenter Plug-in for VMware vSphere	sessions.validate.session
Allow users to access the SnapCenter Plug-in for VMware vSphere	SCV Administrator SCV Backup SCV Guest File Restore SCV Restore SCV View The privilege must be assigned at the vCenter root.

AutoSupport

The SnapCenter Plug-in for VMware vSphere provides a minimum of information for tracking its usage in the NetApp Data Broker virtual appliance, including the plug-in URL. AutoSupport includes a table of installed plug-ins that is displayed by the AutoSupport viewer.

Downloading the NetApp Data Broker OVA (Open Virtual Appliance)

You can download the `.ova` file for the NetApp Data Broker from the NetApp Support Site. The `.ova` file includes a set of microservices for VM and datastore data protection, which are performed by the SnapCenter Plug-in for VMware vSphere, and the NetApp Data Broker, which facilitates the virtual appliance. When the deployment is complete, all components are installed on a Linux VM in your environment.

Before you begin

Attention: The download process does not check for an existing `.ova` file. Therefore, before downloading you must make sure no other NetApp Data Broker `.ova` file exists on the vCenter.

Steps

1. Log in to the NetApp Support Site (<https://mysupport.netapp.com>), and click the **Downloads** tab.
2. On the Downloads page, select **Software**.
3. From the list of products, select **NetApp Data Broker**, then select the **VMware vSphere** platform, and then click **Go!**.
4. Follow the instructions on the product description page until you reach the download page.
5. Download the NetApp Data Broker `.ova` file to any location.

Deploying the NetApp Data Broker virtual appliance

To use SnapCenter features to protect VMs and datastores, you must deploy the NetApp Data Broker virtual appliance.

Before you begin

- You must have read the deployment requirements.
The deployment wizard does not verify the space requirement. If you do not have enough space on the host, the deployment might look successful, but the virtual appliance will not boot up.
- You must be running a supported version of vCenter Server.
- You must have configured and set up your vCenter Server environment.
- You must have set up an ESXi host for your virtual appliance VM.
- You must have downloaded the `NetAppDataBroker.ova` file.
- You must have the login credentials for your vCenter Server instance.
- You must have logged out of and closed all browser sessions of vSphere Web Client and deleted the browser cache to avoid any browser cache issue during the deployment of the virtual appliance.
- You must have enabled Transport Layer Security (TLS) in vCenter. Refer to the VMware documentation.

- You can deploy the NetApp Data Broker virtual appliance in the same vCenter as the virtual appliance for VSC 7.x and later.
- If you plan to perform backups in vCenters other than the one in which the virtual appliance is deployed, the ESXi server, the virtual appliance, and each vCenter must be synchronized to the same time.

Best practice: Deploy the NetApp Data Broker virtual appliance in the same time zone as the vCenter. Backup schedules are executed in the time zone in which the virtual appliance is deployed. vCenter reports data in the time zone in which the vCenter is located. Therefore, if the virtual appliance and the vCenter are in different time zones, data in the SnapCenter Plug-in for VMware vSphere Dashboard might not be the same as the data in the reports.

Steps

1. In your browser, navigate to VMware vSphere vCenter.
2. On the VMware screen, click **vSphere Web Client (Flex)**.
3. Log in to the **VMware vCenter Single Sign-On** page.
4. On the Navigator pane, right-click any inventory object that is a valid parent object of a virtual machine, such as a datacenter, folder, cluster, or host, and select **Deploy OVF Template** to start the VMware deploy wizard.
5. On the **Select an OVF template** page, specify the location of the `NetAppDataBroker.ova` file and click **Next**.

If you downloaded the .ova file to...	Do this...
An internet location	Enter the URL. Supported URL sources are HTTP and HTTPS.
A local file	Click Choose Files and navigate to the .ova file.

6. On the **Select a name and folder** page, enter a unique name for the VM or vApp, and select a deployment location, and then click **Next**.

This step specifies where to import the .ova file into vCenter. The default name for the VM is the same as the name of the selected .ova file. If you change the default name, choose a name that is unique within each vCenter Server virtual machine folder.

The default deployment location for the VM is the inventory object where you started the wizard.

7. On the **Select a compute resource** page, select a resource where you want to run the deployed VM template, and click **Next**.
8. On the **Review details** page, verify the .ova template details and click **Next**.
9. On the **License agreements** page, select the checkbox for **I accept all license agreements**.
10. On the **Select storage** page, define where and how to store the files for the deployed OVF template.
 - a. Select the disk format for the VMDKs.
 - b. Select a VM Storage Policy.

This option is available only if storage policies are enabled on the destination resource.
 - c. Select a datastore to store the deployed OVA template.

The configuration file and virtual disk files are stored on the datastore.

Select a datastore large enough to accommodate the virtual machine or vApp and all associated virtual disk files.

11. On the **Select networks** page, select a source network and map it to a destination network, and then click **Next**.

The Source Network column lists all networks that are defined in the OVA template.

12. On the **Customize template** page, do the following:
 - a. In **Register to existing vCenter**, enter the vCenter credentials.
 - b. In **Create NetApp Data Broker credentials**, enter the NetApp Data Broker credentials.

Attention: Be sure to make a note of the username and password that you specify. You need to use these credentials if you want to modify the virtual appliance configuration at a later time.

- c. In **Setup Network Properties**, enter the network information.
 - d. In **Setup Date and Time**, select the time zone where the vCenter is located.
13. On the **Ready to complete** page, review the page and click **Finish**.

Note: Make sure all hosts are configured with IP addresses (FQDN hostnames are not supported). The deploy operation does not validate your input before deploying.

You can view the progress of the deployment from the Recent Tasks window while you wait for the OVF import and deployment tasks to finish.

When the virtual appliance is successfully deployed, it is deployed as a Linux VM, registered with vCenter, and a SnapCenter vSphere web client is installed.

14. Navigate to the VM where the virtual appliance was deployed, then click the **Summary** tab, and then click the **Power On** box to start the virtual appliance.
15. While the virtual appliance is powering on, right-click the deployed virtual appliance and then click **Install VMware tools**.


The VMware Tools is installed on the VM where the virtual appliance is deployed. For more information on installing VMware Tools, see the VMware documentation.

The deployment might take a few minutes to complete. A successful deployment is indicated when the virtual appliance is powered on, the VMware tools are installed, and the screen prompts you to log in to the NetApp Data Broker.

The screen displays the IP address where the NetApp Data Broker virtual appliance is deployed. Make a note of that location. You will need to log in to the NetApp Data Broker UI if you want to make changes to the virtual appliance configuration.

16. Log in to NetApp Data Broker using the IP address displayed on the deployment screen and the credentials that you provided in the deployment wizard, then verify on the Dashboard that the virtual appliance is successfully connected to vCenter and the SnapCenter Plug-in for VMware vSphere is successfully enabled and connected.

The maintenance console user name is set to "maint" and the password is set to "admin123" by default.

17. Log in to vCenter, then right-click  (home) in the toolbar, and then select **SnapCenter Plug-in for VMware vSphere**.

After you finish

If you are a new SnapCenter user, you must add SVMs before you can perform any data protection operations.

If you are an existing SnapCenter user, you must migrate your existing SnapCenter VM and datastore backups and metadata.

Creating a virtual appliance credential for migrating backups

If you are a SnapCenter customer and have VM consistent or VM crash-consistent backups, or application-consistent backups of virtualized data, you must migrate those backups to the virtual appliance for SnapCenter Plug-in for VMware vSphere. Before migrating, you must add the virtual appliance credentials to SnapCenter Server.

Before you begin

- You must be running SnapCenter Server 4.2.
- You must have deployed the NetApp Data Broker virtual appliance and enabled the SnapCenter Plug-in for VMware vSphere.

Steps

1. In the left navigation pane of the SnapCenter GUI, click **Settings**.
2. In the Settings page, click **Credentials**, and then click **New** to start the wizard.
3. Enter the credential information:

For this field...	Do this...
Credential name	Enter a name for the credentials.
Username	Enter the username specified when the virtual appliance was deployed.
Password	Enter the password specified when the virtual appliance was deployed.
Authentication	Select Linux .

Registering the SnapCenter Plug-in for VMware vSphere with SnapCenter Server

If you want to perform application-over-VMDK workflows in SnapCenter (application-based protection workflows for virtualized databases and file systems), you must register the SnapCenter Plug-in for VMware vSphere virtual appliance with the SnapCenter Server.

Note: If you are a SnapCenter user and you upgraded to SnapCenter 4.2 and migrated your application over VMDK backups to the SnapCenter Plug-in for VMware, the migration command automatically registers the plug-in.

Before you begin

- You must be running SnapCenter Server 4.2.
- You must have deployed the NetApp Data Broker virtual appliance and enabled the SnapCenter Plug-in for VMware vSphere.

About this task

- You register the SnapCenter Plug-in for VMware vSphere with SnapCenter Server by using the SnapCenter GUI to add a “vsphere” type host.

Port 8144 is predefined for communication within the NetApp Data Broker virtual appliance.

Attention: You can register multiple instances of the SnapCenter Plug-in for VMware vSphere on the same SnapCenter Server 4.2 to support application-based data protection operations on VMs. You cannot register the same SnapCenter Plug-in for VMware vSphere on multiple SnapCenter Servers.

- For vCenters in Linked Mode, you must register the SnapCenter Plug-in for VMware vSphere virtual appliance for each vCenter.

Steps

1. In the SnapCenter GUI left navigation pane, click **Hosts**.
2. Verify that the **Managed Hosts** tab is selected at the top.
3. Click **+Add** to start the wizard.
4. On the **Add Hosts** dialog box, specify the host you want to add to the SnapCenter Server:

For this field...	Do this...
Host Type	Select " vSphere " as the type of host.
Host name	Enter the IP address of the NetApp Data Broker virtual appliance.
Credential	Enter the username and password for the NetApp Data Broker virtual appliance that was provided during the appliance deployment.

5. Click **Submit**.
When the VM host is successfully added, it is displayed on the Managed Hosts tab.
6. In the left navigation pane, click **Settings**, then click the **Credential** tab, and then click **+Add** to add credentials for the virtual appliance.
7. Provide the credential information that was specified during the deployment of the NetApp Data Broker virtual appliance.

Note: You must select **Linux** for the Authentication field.

After you finish

If the NetApp Data Broker virtual appliance credentials are modified, you must update the registration in SnapCenter Server using the SnapCenter Managed Hosts page.

Logging in to the SnapCenter VMware vSphere web client

When the NetApp Data Broker virtual appliance is deployed, it installs a SnapCenter vSphere web client, which is displayed on the vCenter screen with other vSphere web clients.


Before you begin

Transport Layer Security (TLS) must be enabled in vCenter. Refer to the VMware documentation.

Steps

1. In your browser, navigate to VMware vSphere vCenter.
2. On the VMware screen, click **vSphere Web Client (Flex)** or **vSphere Client (HTML5)**.
3. Log in to the **VMware vCenter Single Sign-On** page.

Attention: Click the **Login** button. Due to a known VMware issue, do not use the ENTER key to log in. For details, see the VMware documentation on ESXi Embedded Host Client issues.

4. On the **VMware vSphere Web Client** page, click  (home) in the toolbar, and then select **SnapCenter Plug-in for VMware vSphere**.

When to use the SnapCenter GUI and the SnapCenter vSphere web client

The SnapCenter Plug-in for VMware vSphere is different from other SnapCenter plug-ins because you use the web client GUI in vCenter for all backup and restore operations for VMs, VMDKs, and datastores. For all other SnapCenter plug-ins (application-based plug-ins), you use the SnapCenter GUI for backup and restore operations. You can also use the vSphere web client GUI Dashboard to monitor the list of protected and unprotected VMs.

Note: The plug-in supports the vSphere web client. It does not support vCenter thick clients.

To protect VMs and datastores, you use the SnapCenter vSphere web client interface. The web client GUI integrates with NetApp Snapshot copy technology on the storage system. This enables you to back up VMs and datastores in seconds and restore VMs without taking an ESXi host offline.

Use this GUI...	To perform these operations...	And to access these backups...
SnapCenter vSphere web client GUI	VM and datastore backup VMDK attach and detach Datastore mount and unmount VM restore VMDK restore Guest file and folder restore	Backups of VMs and datastores that were performed by using the SnapCenter vSphere web client GUI.
SnapCenter GUI	Backup and restore of virtualized databases and applications, including protecting Microsoft SQL Server databases, Microsoft Exchange databases, SAP HANA databases, and Oracle databases. Database clone	Backups performed by using the SnapCenter GUI.

Note: For VM consistent backup and restore operations, you must use the SnapCenter vSphere web client GUI. Although it is possible to perform some operations using VMware tools, for example, mounting or renaming a datastore, those operations will not be registered in the SnapCenter repository and, therefore, will not be recognized.

Note: SnapCenter does not support single Snapshot copies of databases and VMs together. Backups for VMs and databases must be scheduled and run independently, which creates separate Snapshot copies, even if the databases and VMs are hosted in the same volume. Application backups must be scheduled by using the SnapCenter GUI; VM and datastore backups must be scheduled by using the SnapCenter vSphere web client GUI.

Managing the NetApp Data Broker virtual appliance

You need to use the NetApp Data Broker virtual appliance UI to update the virtual appliance configuration, which includes vCenter credentials, NetApp Data Broker credentials, or time zones for backups.

Modifying the time zone for backups

When you configure a backup schedule for a SnapCenter Plug-in for VMware vSphere resource group, the schedule is automatically set for the time zone in which the NetApp Data Broker virtual appliance is deployed. You can modify that time zone by using the NetApp Data Broker UI.

Before you begin


You must know the IP address and the log in credentials for the NetApp Data Broker.

- The IP address was displayed when the NetApp Data Broker was deployed.
- Use the log in credentials provided during the deployment of the virtual appliance or as later modified.

Steps

1. Log in to the NetApp Data Broker.

Use the format `https://<OVA-IP-address>:8080` to access the NetApp Data Broker.

2. Click the Settings icon in the top toolbar.
3. On the **Settings** page, in the **Date and Time** section, click  **Edit**.
4. Select the new time zone and click **Save**.

The new time zone will be used for all backups performed by the SnapCenter Plug-in for VMware vSphere.

Modifying the NetApp Data Broker logon credentials

You can modify the logon credentials for the NetApp Data Broker. This affects only logging in to the NetApp Data Broker UI.

Before you begin


You must know the IP address and the log in credentials for the NetApp Data Broker.

- The IP address was displayed when the NetApp Data Broker was deployed.
- Use the log in credentials provided during the deployment of the virtual appliance or as later modified.

Steps

1. Log in to the NetApp Data Broker.

Use the format `https://<OVA-IP-address>:8080` to access the NetApp Data Broker.

2. Click the Settings icon in the top toolbar.
3. On the **Settings** page, in the **User** section, click  **Edit**.

4. Enter the new user name or password and click **Save**.

Modifying the vCenter logon credentials in the NetApp Data Broker

You can modify the vCenter logon credentials that are configured in the NetApp Data Broker. These credentials are used by the virtual appliance to access vCenter.

Before you begin


You must know the IP address and the log in credentials for the NetApp Data Broker.

- The IP address was displayed when the NetApp Data Broker was deployed.
- Use the log in credentials provided during the deployment of the virtual appliance or as later modified.

Steps

1. Log in to the NetApp Data Broker.

Use the format `https://<OVA-IP-address>:8080` to access the NetApp Data Broker.

2. In the left navigation pane, click **Configuration**.
3. On the **Configuration** page, in the **vCenter** section, click  **Edit**.
4. Enter the new user name or password and then click **Save**.
Do not modify the port number.

Migrating to the virtual appliance for SnapCenter Plug-in for VMware vSphere

You use Windows PowerShell cmdlets to migrate SnapCenter metadata from the Windows-based SnapCenter Server to the SnapCenter Plug-in for VMware vSphere enabled by the virtual appliance.

There are two migration options:

- Migrating from SnapCenter to the NetApp Data Broker virtual appliance for SnapCenter Plug-in for VMware vSphere

You must migrate metadata for the following from Windows-based SnapCenter:

- VM-consistent data protection performed by the SnapCenter Plug-in for VMware vSphere
- Application-consistent data protection metadata of virtualized databases or file systems performed by a SnapCenter application-based plug-in with support from the SnapCenter Plug-in for VMware vSphere

To migrate, you use the Windows SnapCenter PowerShell cmdlet `invoke-SCVOVAMigration`.

You can only migrate metadata from SnapCenter 4.0 or later.

- Migrating from VSC to the NetApp Data Broker virtual appliance for SnapCenter Plug-in for VMware vSphere

You can migrate VSC 6.2.x (SMVI) metadata for backup jobs that are not integrated with SnapCenter

To migrate, you use the *NetApp Import Utility for SnapCenter and Virtual Storage Console* that is in the NetApp Support ToolChest. Make sure to select the VSC to SnapCenter migration option.

[NetApp ToolChest: NetApp Import Utility for SnapCenter and Virtual Storage Console](#)

Migrating from SnapCenter to the virtual appliance for SnapCenter Plug-in for VMware vSphere

You use the SnapCenter Windows PowerShell cmdlets to migrate SnapCenter VM-consistent backup metadata and SnapCenter application-consistent for virtualized data backup metadata to the NetApp Data Broker virtual appliance for SnapCenter Plug-in for VMware vSphere.

Before you begin

- You must be running SnapCenter Server 4.2 or later.
- The NetApp Data Broker virtual appliance must be deployed with SnapCenter Plug-in for VMware vSphere enabled, registered on vCenter, and registered on SnapCenter Server.
- On the NetApp Data Broker dashboard, the status for SnapCenter Plug-in for VMware vSphere must be “connected.”
- You must have created a Linux virtual appliance credential for migrating backups.
- SnapCenter hosts must be configured with IP addresses, not fully qualified domain names (FQDN).

Note: In a Linked Mode environment, you must migrate all linked nodes together.

- Names for SVMs must resolve to management LIFs.
If you added etc host entries for SVM names in SnapCenter, you must verify that they are also resolvable from the virtual appliance.

About this task

- The migration command migrates metadata from SnapCenter 4.0, 4.1, and 4.1.1 only. If you are using an earlier version of SnapCenter then you must first upgrade before you can migrate.
 - What is migrated:
 - SnapCenter metadata, which includes storage systems, customized throttles and email settings in the SnapCenter configuration file, policies, resource groups, backup metadata, and mounts.
 - What is not migrated:
 - Pre- and post-scripts that are configured for resource groups
 - Active guest file restore sessions, guest file restore credentials, and proxy VMs
 - `scbr.override` configuration file
- You must use the Windows Powershell cmdlet `invoke-SCVOVAMigration` for each SnapCenter Plug-in for VMware vSphere that is registered with SnapCenter. The cmdlet does the following:
 - Suspends all schedules to prevent job failures during the migration. After a successful migration, schedules are automatically re-enabled.
 - Migrates storage connections and metadata.
 - Creates backup schedules for post-migration backups.
 - Uninstalls the existing SnapCenter Plug-in for VMware vSphere from the Windows host.
 - Removes the vSphere host and resource groups from the Windows SnapCenter Server.
 - Activates the backups jobs on the virtual appliance for SnapCenter Plug-in for VMware vSphere.
 - Registers the vSphere host for the virtual appliance with SnapCenter to support application-based backups of virtualized databases and file systems (application over VMDK backups).
- Metadata for application-based VMDK backups is stored in the SnapCenter Server repository. Metadata for VM and datastore backups is stored in the NetApp Data Broker virtual appliance repository.

Steps

1. Log on to the SnapCenter vSphere web client and verify that no jobs are running.
2. Log on to the SnapCenter GUI using the SnapCenter Admin username.
If you use any other username to log in, even if that username has all permissions, a migration error might occur.
3. In the Windows SnapCenter GUI left navigation pane, click **Settings**, then click the **Credential** tab, and then click **+Add** to add credentials for the virtual appliance.
4. Provide the credential information that was specified during the deployment of the NetApp Data Broker virtual appliance.

Note: You must select **Linux** for the Authentication field.

This step adds the credentials that SnapCenter Server uses to access the virtual appliance during the migration.

5. Open a Windows PowerShell window and run the following cmdlets:

Open-SmConnection

```
invoke-SCVOVAMigration -SourceSCVHost old-SCV-host-IP
-DestinationSCVOVAHost new-OVA-IP -OVACredential OVA-credentials
-ByPassValidationCheck -Overwrite -ContinueMigrationOnStorageError
-ScheduleOffsetTime time-offset
```

The migration command suspends job schedules before migrating metadata and registers the virtual appliance with SnapCenter Server.

After you finish

- Job details on the Dashboard
Information on the migrated backups is listed in the recent jobs but detailed information is not displayed in the Dashboard until backups are performed after the migration.
- Backup names
Backup names before migration have the format `RGName_HostName_Timestamp`.
For example, `-NAS_DS_RG_perflserver_07-05-2019_02.11.59.9338`.
Backup names after migration have the format `RGName_Timestamp`.
For example, `-NAS_VM_RG_07-07-2019_21.20.00.0609`.
- Pre- and post-scripts
Scripts that are configured for resource groups are not migrated. In addition, scripts written for Windows systems will not run on the Linux-based virtual appliance. Therefore, you must recreate the scripts and add those scripts after migration.
- Guest file restore credentials
Guest file restore credentials are not migrated. Therefore, you must create new guest file credentials after the migration.
- `scbr.override` configuration file
If you have customized settings in the `scbr.override` configuration file, then you must move that file to the virtual appliance and restart the web client service.
- Upgrade SnapCenter plug-ins
If you use the virtual appliance for SnapCenter Plug-in for VMware vSphere to support other SnapCenter plug-ins, then you must update those plug-ins to 4.2 or later.
- Suspended SnapCenter application-based plug-ins
If you manually suspended a SnapCenter application-based plug-in before the migration, the migration process automatically restarts the plug-in.
- Uninstall SnapCenter Server
If you use SnapCenter *only* for VM-consistent or crash-consistent data protection, then after all VM backups are migrated to the virtual appliance, you can uninstall SnapCenter Server on the Windows host.

Accessing the maintenance console

You can manage your application, system, and network configurations by using the maintenance console of the virtual appliance for SnapCenter Plug-in for VMware vSphere that is provided by NetApp Data Broker. You can change your administrator password and maintenance password by using the maintenance console. You can also generate support bundles and start remote diagnostics by using the maintenance console.


Before you begin

Before stopping and restarting the NetApp Data Broker service, you should suspend all schedules.

About this task

- You must use “maint” as the user name and “admin123” as the password to log in to the maintenance console of the NetApp Data Broker appliance.
- You must set a password for the “diag” user while enabling remote diagnostics.
To obtain the root user permission to execute the command, use `sudo <command>`.

Steps

1. Access the **Summary** tab of the virtual appliance and then click  to start the maintenance console.

You can access the following maintenance console options:

Category	Available maintenance options
Application Configuration	Display NetApp Data Broker summary Start or stop NetApp Data Broker service Change username or password for NetApp Data Broker login Change MySQL password Configure MySQL backup List MySQL backups Restore MySQL backup
System Configuration	Reboot or shutdown virtual machine Change 'maint' user password Change time zone Change NTP server Enable/Disable SSH Access Increase jail disk size (/jail) Upgrade Install VMware Tools
Network Configuration	Display or change IP address settings Display or change domain name search settings Display or change static routes Commit changes Ping a host
Support and Diagnostics	Generate support bundle Access diagnostic shell Enable remote diagnostic access Generate core dump bundle

Disabling the SnapCenter Plug-in for VMware vSphere

If you no longer need the SnapCenter data protection features, you must change the configuration of the NetApp Data Broker virtual appliance. For example, if you deployed the NetApp Data Broker virtual appliance in a test environment, you might need to disable the SnapCenter features in that environment and enable them in a production environment.

Before you begin

- You must have administrator privileges.

Steps

1. Optional: Back up the SnapCenter MySQL repository in case you want to restore it to a new virtual appliance.
[Backing up the virtual appliance repository](#)
2. Log in to NetApp Data Broker web client.
The IP of the NetApp Data Broker is displayed when you deploy the virtual appliance.
3. Click **Configuration** in the left navigation pane, and then click the service option for **SnapCenter Plug-in for VMware vSphere** to disable the plug-in.
4. Confirm your choice.
 - If you only used SnapCenter Plug-in for VMware vSphere to perform VM consistent backups
The plug-in is disabled, and no further action is required.
 - If you used SnapCenter Plug-in for VMware vSphere to perform application-consistent backups
The plug-in is disabled, and further cleanup is required.
 - a. Log in to VMware vSphere.
 - b. In the left navigator screen, right-click the instance of the OVA (the name of the OVA that was used when the OVA was deployed) and select **Delete from Disk**.
 - c. Log in to SnapCenter and remove the vSphere host.

Removing the SnapCenter Plug-in for VMware vSphere

If you no longer need to use the SnapCenter data protection features, you must disable the plug-in to unregister it from Vcenter, then remove the plug-in from vCenter, then manually delete leftover files.

Before you begin

- You must have administrator privileges.

Steps

1. Log in to NetApp Data Broker web client.
The IP of the NetApp Data Broker is displayed when you deploy the virtual appliance.
2. Click **Configuration** in the left navigation pane, and then click the service option for **SnapCenter Plug-in for VMware vSphere** to disable the plug-in.
3. Log in to VMware vSphere.
4. In the left navigator screen, right-click the instance of the OVA (the name of the OVA that was used when the OVA was deployed) and select **Delete from Disk**.
5. Manually delete the following files in the pickup folder of the vCenter server:
`vsc-httpclient3-security.jar`
`scv-api-model.jar`
`scvm_webui_service.jar`
`scvm_webui_ui.war`
`gson-2.5.jar`
6. If you used the plug-in to support other SnapCenter plug-ins for application-consistent backups, log in to SnapCenter and remove the vSphere host.

After you finish

The NetApp Data Broker virtual appliance is still deployed but the SnapCenter Plug-in for VMware vSphere is removed.

Troubleshooting

If you encounter unexpected behavior while performing data protection operations using the VMware vSphere web client for the SnapCenter Plug-in for VMware vSphere, you can use the log files to identify the cause and resolve the problem.

For detailed information on any SnapCenter Plug-in for VMware vSphere operation, you can use the plug-in Dashboard to download the VMware vSphere web client log files.

vCenter MOB entry for the SnapCenter plug-in is not updated

Description

After deploying the virtual appliance .ova, the MOB entry in vCenter for the SnapCenter Plug-in for VMware vSphere still shows the old version number. This can occur when other jobs are running in the vCenter. vCenter will eventually update the entry.

Corrective action

No corrective action required.

VMware vSphere web client GUI not working correctly

Description

After a deployment, or after an upgrade on a VM where Virtual Storage Console for VMware vSphere (VSC) was previously installed, the following might occur:

- Right-click menus that are documented for mount, unmount, attach, and detach operations do not appear.
- The SnapCenter VMware vSphere web client GUI does not match the documentation.
- The Dashboard is not displayed correctly.

During normal use, a page display (for example, the Resource Groups page) might stall or get stuck loading.

Corrective action

1. Clear the browser cache and then check if the GUI is operating properly.
2. If the problem persists, then restart the VMware vSphere web client service.

Restarting the vSphere web client service in Linux

If your vCenter is on a Linux appliance, then you must use Linux commands to restart the VMware web client service.

Steps

1. Use SSH to log in to the vCenter Server Appliance as root.
2. Access the Appliance Shell or BASH Shell by using the following command:

```
shell
```

3. Stop the web client service by using the following command:

Client	Command
Flex	<code>service-control --stop vsphere-client</code>
HTML5	<code>service-control --stop vsphere-ui</code>

4. Delete all stale `scvm` packages on vCenter by using the following command:

Client	Command
Flex	<code>etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity/ rm -rf com.netapp.scvm.webclient-<version_number></code>
HTML5	<code>etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity/ rm -rf com.netapp.scvm.webclient-<version_number></code>

Attention: Do not remove the VASA or VSC7.x and later packages.

5. Start the web client service by using the following command:

Client	Command
Flex	<code>service-control --start vsphere-client</code>
HTML5	<code>service-control --start vsphere-ui</code>

Restarting the vSphere web client service in Windows

If your vCenter is on a Windows host, then you must use Windows commands to restart the VMware web client service.

Steps

1. If you are running vCenter 6.5 or later, perform the following:

- a) Stop the web client service by using the following command:

Client	Command
Flex	<code>service-control --stop vsphere-client</code>
HTML5	<code>service-control --stop vsphere-ui</code>

Wait for the message `Completed Stop service request`.

- b) Delete all stale `scvm` packages on vCenter by performing the following:

- i. Navigate to the vCenter `vsphere-client-serenity/` folder.

Client	Location of folder
Flex	<code>C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\ vc-packages\vsphere-client-serenity\</code>
HTML5	<code>C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\ vc-packages\vsphere-client-serenity\</code>

- ii. Delete all plug-in folders with the following name:
`com.netapp.scvm.webclient-<version_number>`.

- c) Restart the web client service by using the following command:

Client	Command
Flex	<code>service-control --start vsphere-client</code>
HTML5	<code>service-control --start vsphere-ui</code>

Wait for the message `Completed Start service request`.

2. If you are running vCenter 6.0 update 3 or later, perform the following:

- Open Server Manager on the Windows system on which vCenter Server is running.
- Click **Configuration > Services**.
- Select **VMware vSphere Web Client** and click **Stop**.
- Delete all stale packages on vCenter by performing the following:

- i. Navigate to the vCenter `vsphere-client-serenity/` folder.

Client	Location of folder
Flex	<p>vCenter Server Appliance: <code>etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity/</code></p> <p>vCenter Server for Windows: <code>C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity\</code></p> <p>Mac OS: <code>/var/lib/vmware/vsphere-client/vsphere-client/vc-packages/vsphere-client-serenity/</code></p>
HTML5	<p>vCenter Server Appliance: <code>etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity/</code></p> <p>vCenter Server for Windows: <code>C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-serenity\</code></p> <p>Mac OS: <code>/var/lib/vmware/vsphere-ui/vsphere-client/vc-packages/vsphere-client-serenity/</code></p>

- ii. Delete all plug-in folders with the following name:
`com.netapp.scvm.webclient-<version_number>`.

- e) Select **VMware vSphere Web Client** and click **Start**.

Authentication error

Description

You encountered an authentication error either after deploying NetApp Data Broker or when performing a migration. This occurs when the credentials you used are not Admin.

Corrective action

1. Log on to the NetApp Data Broker GUI using the format <https://<OVA-IP-address>:8080>.
2. Restart the service.

Bad gateway error

Description

One reason this error occurs is if you manually added files or other content to the NetApp Data Broker appliance and then tried to migrate. In this scenario, there is not enough space in the appliance for the migration process.

Error message

The remote server returned an error: (502) Bad Gateway.

Corrective action

Remove any manually-added files.

Cannot download job logs

Description

You tried to download job logs, but the log file named in the error message has been deleted.

Error message

```
HTTP ERROR 500 Problem accessing /export-scv-logs.
```

Corrective action

Check the file access status and permissions for the file named in the error message and correct the access problem.

Cannot unmount a backup

Description

Although the backup is listed as mounted in the SnapCenter VMware vSphere web client GUI, it is not listed in the unmount backup screen.

Workaround

Use the REST API `"/backup/{backup-Id}/cleanup"` to clean up the out-of-bound datastores.

You may have reached the maximum number of NFS volumes configured in the vCenter

Description

You attempted to mount a backup copy of an NFS datastore on a storage virtual machine (SVM) with the root volume in a load-sharing mirror relationship.

Error message

```
You may have reached the maximum number of NFS volumes configured in the vCenter. Check the vSphere Client for any error messages.
```

Corrective action

To prevent this problem, change the maximum volumes setting by navigating to **ESX > Manage > Settings > Advance System Settings** and changing the NFS.MaxVolumes value. Maximum value is 256.

Unable to discover datastores on an SVM without a management LIF

Description

A scheduled backup job failed when a storage virtual machine (SVM) without a management LIF was added in the virtual appliance for SnapCenter Plug-in for VMware vSphere. The plug-in cannot resolve this SVM and was unable to discover any datastores or volumes on the SVM on which to perform backup or restore operations.

Corrective action

Either enable the management LIF before you can perform backup or restore operations, or add a cluster that contains the SVM.

Plug-in is still listed in vCenter after being removed**Description**

After removing the virtual appliance for SnapCenter Plug-in for VMware vSphere host VM, the plug-in remains listed in vCenter until the local vCenter cache is refreshed. However, because the plug-in was removed, no SnapCenter VMware vSphere operations can be performed on that host.

Workaround

Restart the vCenter web client service.

“Bad Gateway” error during migration**Description**

During migration from SnapCenter to the SnapCenter Plug-in for VMware vSphere virtual appliance, the NetApp Data Broker connection was stopped, or the service was stopped.

Workaround

The NetApp Data Broker connection status must be “connected” during the migration process. You can also manually update the time out configuration in the virtual appliance.

Information not displayed after upgrading to a new patch of the same release**Description**

After upgrading the virtual appliance to a new patch of the same release, recent jobs or other information are not displayed in the Dashboard and job monitor.

Before upgrading to a new patch of the same release, you must clear the SnapCenter Plug-in for VMware vSphere cache on the vCenter Web Server and restart the server before the upgrade or registration.

If the plug-in cache is not cleared, then recent jobs are not displayed in the Dashboard and job monitor in the following scenarios:

- The virtual appliance was deployed using vCenter, and then later upgraded to a patch in the same release.
- The virtual appliance was deployed using vCenter 1. Later, this virtual appliance was registered to a new vCenter 2. A new virtual appliance is created with a patch and registered to vCenter 1. However, because vCenter 1 still has the cached plug-in from the first virtual appliance without the patch, the cache needs to be cleared.

The cache is in the following locations, based on the type of server operating system:

- vCenter Server for Windows
`C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity\`
- vCenter Server Appliance

```
/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity/
```

- Windows OS

```
%PROGRAMFILES%/VMware/vSphere Web Client/vc-packages/vsphere-client-serenity/
```

- Mac OS

```
/var/lib/vmware/vsphere-client/vsphere-client/vc-packages/vsphere-client-serenity/
```

Workaround before upgrading

1. Locate the `vsphere-client-serenity` folder, then locate the `com.netapp.scvm.webclient-4.2.0` folder and delete it.

Note: The folder name changes for each release.

2. Restart the vCenter Server.

You can then upgrade the virtual appliance.

Workaround if you already upgraded before clearing the cache

1. Log in to NetApp Data Broker GUI.

The IP of the NetApp Data Broker is displayed when you deploy the virtual appliance.

2. Click **Configuration** in the left navigation pane, and then click the service option for **SnapCenter Plug-in for VMware vSphere** to disable the plug-in.

The plug-in is disabled and the extension is unregistered in vCenter.

3. Locate the `vsphere-client-serenity` folder, then locate the `com.netapp.scvm.webclient-4.2.0` folder and delete it.

Note: The folder name changes for each release.

4. Restart the vCenter Server.

You can then upgrade the virtual appliance.

3. Log in to NetApp Data Broker web client.

4. Click **Configuration** in the left navigation pane, and then click the service option for **SnapCenter Plug-in for VMware vSphere** to enable the plug-in.

The plug-in is enabled and the extension is registered in vCenter.

Resources not available if NetApp Data Broker is stopped in linked vCenter

Description

If you stop the NetApp Data Broker service in a vCenter that is in Linked Mode, resource groups are not available in all the linked vCenters, even when the NetApp Data Broker service is running in the other linked vCenters.

Workaround

Unregister the NetApp Data Broker extensions manually, as follows:

1. On the linked vCenter that has the NetApp Data Broker service stopped, navigate to the Managed Object Reference (MOB) manager.

2. In the Properties option, select Extension Manager to display a list of the registered extensions.
3. Unregister the extensions "com.netapp.scvm.webclient" and "com.netapp.aegis".

Copyright information

Copyright © 2019 NetApp, Inc. All rights reserved. Printed in the U.S.

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

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

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

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

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

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).

Trademark information

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

<http://www.netapp.com/us/legal/netapptmlist.aspx>

How to send your 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., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277