SnapCenter® Software 4.0

Data Protection Guide

For VMs and Datastores using the SnapCenter Plug-in for VMware vSphere®

August 2019 | 215-12931_2019-08_en-us
doccomments@netapp.com

NetApp®

Contents

Deciding whether to read the Data Protection Guide for VMs and Datastores using the SnapCenter Plug-in for VMware vSphere

This guide describes how to use SnapCenter Plug-in for VMware vSphere. The plug-in provides a vSphere web client GUI on vCenter to protect VMware virtual machines (VMs) and datastores. It also supports SnapCenter application-specific plug-ins in protecting virtualized databases and file systems.

You should read this information if you want to use SnapCenter Plug-in for VMware vSphere in the following ways:

- You want to protect virtualized infrastructure (VMs, VMDKs, and datastores), and virtualized applications, databases, and file systems
- You want to perform backup, restore, attach, and detach operations on VMs and VMDKs
- You want to perform backup, mount, and unmount operations on VM datastores
- You want to create SnapCenter data protection policies and resource groups for VMs and datastores
- You want to restore individual files or folders that reside on a VM guest OS

You should have already performed the following:

- Installed SnapCenter Server on a Windows host
- Installed SnapCenter Plug-in for VMware vSphere on either the SnapCenter Server or on a dedicated Windows host.

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

- SnapCenter installation and setup information
  Installing and setting up SnapCenter
- SnapCenter Data Protection Guides for other types of resources, such as Microsoft SQL Server, Oracle, Windows file systems and custom plug-ins
  NetApp SnapCenter Software Resources
- SnapCenter PowerShell commands or Linux commands information
  SnapCenter Software 4.0 Windows Cmdlet Reference Guide
  SnapCenter Software 4.0 Linux Command Reference Guide
- SnapCenter administrative information
  Information on dashboards, reporting capabilities, and managing licenses, storage connections, and the SnapCenter Server repository.
  Performing administrative tasks with SnapCenter
- SnapCenter concepts information, including architecture, features, and benefits
  SnapCenter concepts

SnapCenter Plug-in for VMware vSphere overview

The Plug-in for VMware vSphere is a host-side component of the NetApp storage solution. It provides a vSphere web client GUI on vCenter to protect VMware virtual machines (VMs) and datastores, and supports SnapCenter application-specific plug-ins in protecting virtualized databases and file systems on primary and secondary storage.

- Support for VMs, VMDKs, and datastores

  The Plug-in for VMware vSphere provides a VMware vSphere web client in vCenter. The web client GUI allows you to perform backups of VMs, VMDKs, and datastores. It also allows you to restore VMs, VMDKs, and files and folders that reside on a guest OS.

- Support for virtualized databases and file systems

  The Plug-in for VMware vSphere provides native backup, recovery, and cloning of virtualized applications (virtualized SQL and Oracle databases and Windows file systems) when you use the SnapCenter GUI. SnapCenter natively leverages the Plug-in for VMware vSphere for all SQL, Oracle, and Windows file system data protection operations on virtual machine disks (VMDKs), raw device mappings (RDMs), and NFS datastores.

  To take application-consistent backups of virtualized MS-SQL and Oracle databases, you must deploy Plug-in for VMware vSphere in addition to SnapCenter Plug-in for Microsoft SQL Server or SnapCenter Plug-in for Oracle Database.

  After the Plug-in for VMware vSphere is installed, you do not need to take any further action; the plug-in handles all interaction with vCenter.

  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 web client GUI in vCenter.

  The Plug-in for VMware vSphere supports all virtualized applications that are supported by SnapCenter.

- VMware Storage VMotion feature is required for restore operations in SAN (VMFS) environments

  The restore workflow for VMware file system (VMFS) restore operations 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 ONTAP commands and do not require VMware Storage VMotion.

- The Plug-in for VMware vSphere is installed on a Windows host.

  Although the Plug-in for VMware vSphere must be installed on a Windows host, it supports both Windows-based vCenters and Linux-based vCenter appliances. SnapCenter natively uses this plug-in to communicate with your vCenter for data protection operations of Windows and Linux virtualized applications without user intervention.

- Virtual Storage Console for VMware vSphere (VSC) backup jobs

  If you are using Virtual Storage Console for VMware vSphere (VSC) 6.x or earlier for backup and recovery, you must migrate your backup jobs to the Plug-in for VMware vSphere. In VSC Appliance 7.0 and later, the backup and recovery functionality of VMs, VMDKs, and datastores has been moved to the SnapCenter plug-in. However, you can use the VSC Appliance 7.0 and later for storage management operations.

  There are two migration paths from VSC to the Plug-in for VMware vSphere:

  - If you are using VSC in conjunction with SnapCenter to back up VMs and datastores, you can use the migration feature in the SnapCenter GUI.

  - If you are using VSC with SnapManager for Virtual Infrastructure (SMVI), you can use the *NetApp Import Utility for SnapCenter and Virtual Storage Console* to migrate the backups, backup jobs, and storage connections. The utility is in the NetApp Support Toolchest.
    NetApp ToolChest: NetApp Import Utility for SnapCenter and Virtual Storage Console
- VSC Appliance 7.0
  VSC Appliance 7.0 and later can coexist with SnapCenter Plug-in for VMware vSphere 3.0 and later on the same vCenter instance. However, SnapCenter 3.x and later cannot co-exist with VSC 6.2.x and earlier on the same vCenter instance.
  You use the Plug-in for VMware vSphere to perform backup and restore operations, and you use the VSC Appliance to perform host and storage monitoring, datastore provisioning, and Storage Policy Based Management (SPBM) support.

In addition to these major features, the 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).

NetApp Interoperability Matrix Tool

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 plug-in.

For information about the SnapCenter architecture, features, and benefits, see the SnapCenter concepts documentation.

Related information

SnapCenter concepts
Installing and setting up SnapCenter

When to use the SnapCenter GUI and the vCenter GUI

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 plug-ins, you use the SnapCenter GUI for backup and restore operations. You can also use the Dashboard in the vCenter web client GUI to monitor the list of protected and unprotected VMs.

To work with the Plug-in for VMware vSphere to protect VMs and datastores, you use the VMware vSphere web client interface in vCenter. 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 a host offline.

Use this GUI...	To perform these operations...	And to access these backups...
Plug-in for VMware vSphere GUI in vCenter	VM and datastore backup VMDK attach and detach VM restore VMDK restore Guest file and folder restore	Backups of VMs and datastores performed by using the Plug-in for VMware vSphere GUI in vCenter.
SnapCenter GUI	Backup and restore of virtualized databases and applications, including protecting Microsoft SQL databases and Oracle databases.	Backups performed by using the SnapCenter GUI.

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 web client GUI in vCenter.

Both vCenter and SnapCenter job monitors display all SnapCenter jobs, regardless of which GUI was used to start the job.

Example for protecting a Microsoft SQL Server database that is running on VMs

To perform an application-consistent backup of a Microsoft SQL Server database that is running on VMs, you use the SnapCenter GUI to start a backup of the database.

SnapCenter uses the SnapCenter Plug-in for Microsoft SQL Server and the SnapCenter Plug-in for Microsoft Windows to perform the operation, and uses the Plug-in for VMware vSphere to communicate with vCenter.

You also use the SnapCenter GUI to access or restore the backup.

Example for protecting an Oracle database that is running on VMs

To perform an application-consistent backup of an Oracle database that is running on VMs, you use the SnapCenter GUI to start a backup of the database.

SnapCenter uses the SnapCenter Plug-in for Oracle Database and the SnapCenter Plug-in for UNIX to perform the operation, and uses the Plug-in for VMware vSphere to communicate with vCenter.

You also use the SnapCenter GUI to access or restore the backup.

Example for protecting a VM

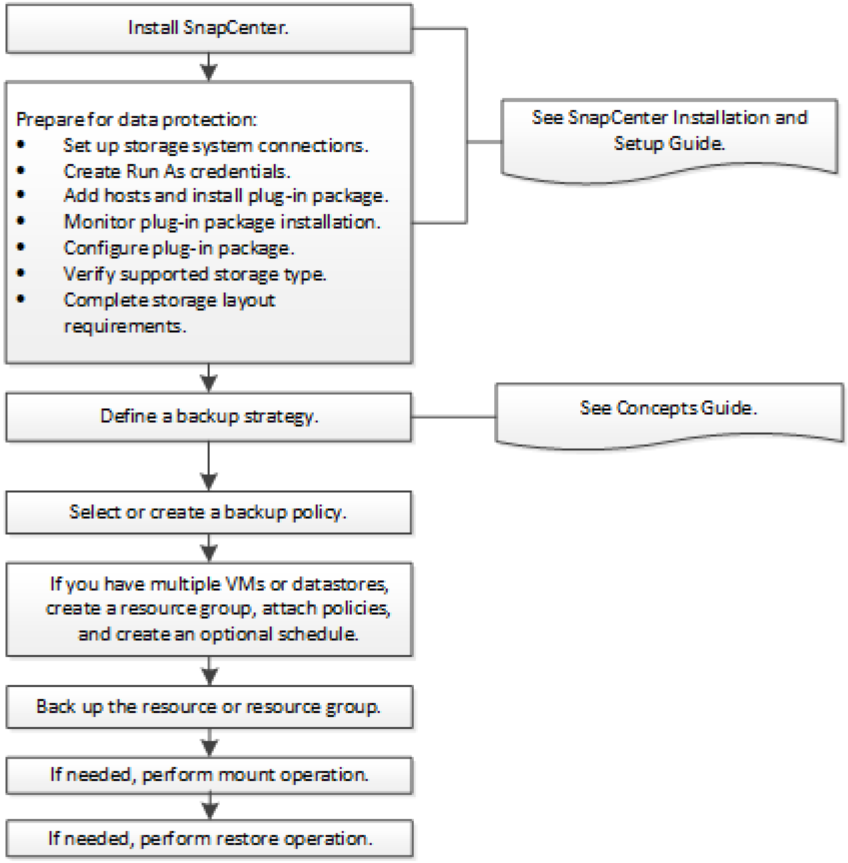
To perform a host-level backup of a VM in which a database application is running (not an application-consistent backup), you use the Plug-in for VMware vSphere GUI in vCenter to start the backup.

SnapCenter uses the Plug-in for VMware vSphere to perform the operation.

You also use the web client GUI in vCenter to access or restore the backup.

SnapCenter Plug-in for VMware vSphere data protection workflow

The data protection workflow lists the tasks that you have to perform for data protection.


Install SnapCenter.
Prepare for data protection:
Set up storage system connections.
Create Run As credentials.
Add hosts and install plug-in package.
Monitor plug-in package installation.
Configure plug-in package.
Verify supported storage type.
Complete storage layout requirements.
See SnapCenter Installation and Setup Guide.
Define a backup strategy.
See Concepts Guide.
Select or create a backup policy.
If you have multiple VMs or datastores, create a resource group, attach policies, and create an optional schedule.
Back up the resource or resource group.
If needed, perform mount operation.
If needed, perform restore operation.

Logging in to SnapCenter

Through SnapCenter role-based access control, users or groups are assigned roles and resources. When you log in to the SnapCenter graphical user interface, you log in with an Active Directory account.

About this task

During the installation, the SnapCenter Server Installation wizard creates a shortcut and places it on the desktop where SnapCenter is installed. Additionally, at the end of the installation, the Install wizard displays the SnapCenter URL based on information you supplied during the installation, which you can copy if you want to log in from a remote system.

> **Attention:** Closing just the SnapCenter browser tab does not log you off of SnapCenter if you have multiple tabs open in your web browser. To end your connection with SnapCenter, you must log off of SnapCenter either by clicking the **Sign out** button or shutting down the entire web browser.
>
> **Attention:** For security reasons, it is recommended not to allow your browser to save your SnapCenter password.

The default GUI URL is a secure connection to the default port 8146 on the server where the SnapCenter Server is installed (https://*server*:8146). If you provided a different server port during the SnapCenter installation, that port is used instead.

For Network Load Balance (NLB) deployment, you must access SnapCenter using the NLB cluster IP (https://*NLB_Cluster_IP*:8146). If you do not see the SnapCenter UI when you navigate to `https://NLB_Cluster_IP:8146` in Internet Explorer (IE), you must add the NLB IP address as a trusted site in IE on each plug-in host, or you must disable IE Enhanced Security on each plug-in host.

NetApp KB Article 2025082: SnapCenter in an HA configuration with Application Request Routing enabled.

Steps

1. Launch SnapCenter from the shortcut located on your local host desktop, from the URL provided at the end of the installation, or from the URL provided to you by your SnapCenter administrator.
2. Enter your user credentials:

   `Domain\UserName`

   > **Note:** If you are logging into SnapCenter for the first time, you must log in using the credentials that you provided during the install process.

3. If you are assigned more than one role, from the **Role** box, select the role you want to use for this login session.

   Your current user and associated role are shown in the upper right of SnapCenter once you are logged in.

Result

If you are using SnapCenter for the first time, the Storage Systems page displays, and the Get Started pane is expanded.

Logging in to the SnapCenter Plug-in for VMware vSphere web client in vCenter

When SnapCenter Plug-in for VMware vSphere is installed, it also provides a VMware vSphere web client, which is displayed on the vCenter screen with the other web clients.

Steps

1. In your browser, navigate to VMware vSphere vCenter.
2. On the VMware screen, click **vSphere Web Client (Flash)**.
3. On the **VMware vCenter Single Sign-On** page, log on.
4. On the **VMware vSphere Web Client** page, click 🏠 in the toolbar and select **SnapCenter Plug-in for VMware vSphere** or click **SnapCenter Plug-in for VMware vSphere** in the left Navigator pane.

Preparing for data protection for VMs, VMDKs, and datastores

Before performing any data protection operation such as backup or restore operations, you must define your strategy and set up the SnapCenter and vCenter environment. Using SnapCenter and SnapCenter Plug-in for VMware vSphere policies, you can perform SnapMirror and SnapVault updates.

To take advantage of SnapVault and SnapMirror technology, you must configure and initialize a data protection relationship between the source and destination volumes on the storage device. You can use NetApp OnCommand System Manager or you can use the ONTAP storage console command line to perform these tasks.

Note: You define SnapVault and SnapMirror relationships between source and destination volumes outside the SnapCenter Plug-in for VMware vSphere. For information on defining these relationships, see the ONTAP data protection documentation.

Data Protection Power Guide

Prerequisites for using SnapCenter Plug-in for VMware vSphere

Before using SnapCenter Plug-in for VMware vSphere and this user guide, the following tasks should be completed. See the installation information for detailed information.

- Verify that all proper licenses are installed on the NetApp storage systems, including those that are used at the sources and destinations of SnapMirror and SnapVault relationships.
- Add RBAC roles to SnapCenter users and assign permissions to resources, including permissions for secondary (destination) resources if you are using SnapMirror or SnapVault.
- Configure the SnapCenter environment by adding SVM connections.

  Note: SnapCenter does not support cluster connections, only individual SVMs. SnapCenter does not support multiple SVMs with the same name on different clusters. Each SVM supported by SnapCenter must have a unique name.
- Create Run As credentials.
  - The SnapCenter admin role must have admin privileges.
  - Although Run As credentials are not needed for scheduling jobs (except if you are using a SQL scheduler with SnapCenter Plug-in for Microsoft Windows), they are needed when you upgrade or uninstall SnapCenter Plug-in for VMware vSphere from the SnapCenter Server. If you originally installed the plug-in from the SnapCenter GUI, then you already configured Run As credentials. However, if you manually installed SnapCenter Plug-in for VMware vSphere, then you must configure Run As credentials. See the installation information.
- Install the plug-in, add VM hosts, discover (refresh) the resources, and configure the plug-in.
- Set up SnapMirror and SnapVault relationships, if you want backup replication.

Related information

Installing and setting up SnapCenter

Configuring SnapCenter Plug-in for VMware vSphere for email alerts

You can configure the Plug-in for VMware vSphere to send email alerts on the status of VM and datastore data protection operations when jobs are executed.

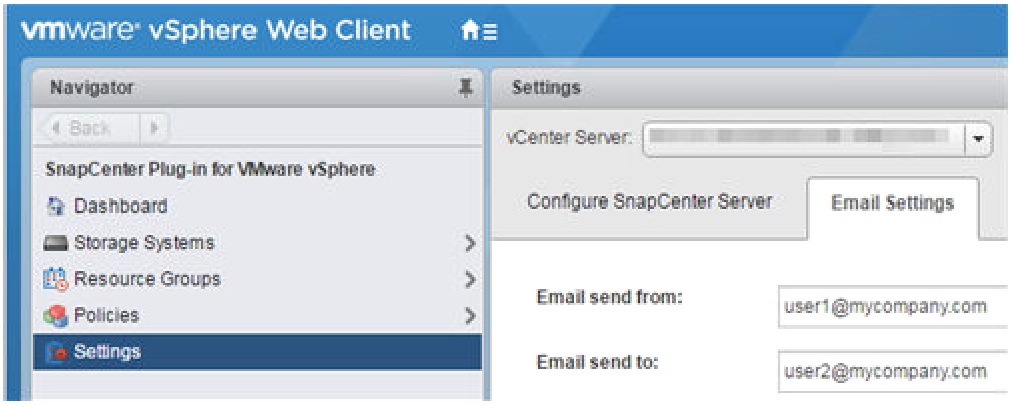
About this task

You can configure the default email alert settings that are applied when you create resource groups. The default settings can be modified when a resource group is created.

> **Note:** The SMTP server address is saved in the SnapCenter Server repository as a global setting for all SnapCenter plug-ins, not just SnapCenter Plug-in for VMware vSphere.

Steps

1. In the left Navigator pane of the VMware vSphere web client in vCenter for the Plug-in for VMware vSphere, click **Settings**, and then click the **Email Settings** tab.



Email send from: user1@mycompany.com

Email send to: user2@mycompany.com

2. Provide the information, as follows:

For this field…	Do this…
Email send from	Email from address
Email send to	Email to address Enter one or more valid email addresses, separated by commas.
SMTP Server	Address of the SMTP server For example: `smtp.abc.testlab.mycompany.com`

3. Optional: Click **Test email settings**.

   This option sends a test email using the information you just entered.

4. Click **Confirm** to save the configuration.

Role-based access control for SnapCenter Plug-in for VMware vSphere

SnapCenter Plug-in for VMware vSphere provides an additional level of RBAC for managing virtualized resources. SnapCenter Plug-in for VMware vSphere supports both vCenter Server RBAC and Data ONTAP RBAC.

The Plug-in for VMware vSphere ships with predefined vCenter roles. You must add these roles to vCenter Active Directory users to perform SnapCenter operations on the vCenter GUI. You cannot change the permissions of the SnapCenterAdmin role.

You can create and modify roles, and add resource access to users at any time. However, when you are setting up SnapCenter and the Plug-in for VMware vSphere for the first time, you should at least add Active Directory users or groups to roles, and then add resource access to those users or groups.

Note that user or group accounts are not created using SnapCenter, but are created in the Active Directory in the operating system or database.

Types of RBAC for SnapCenter Plug-in for VMware vSphere users

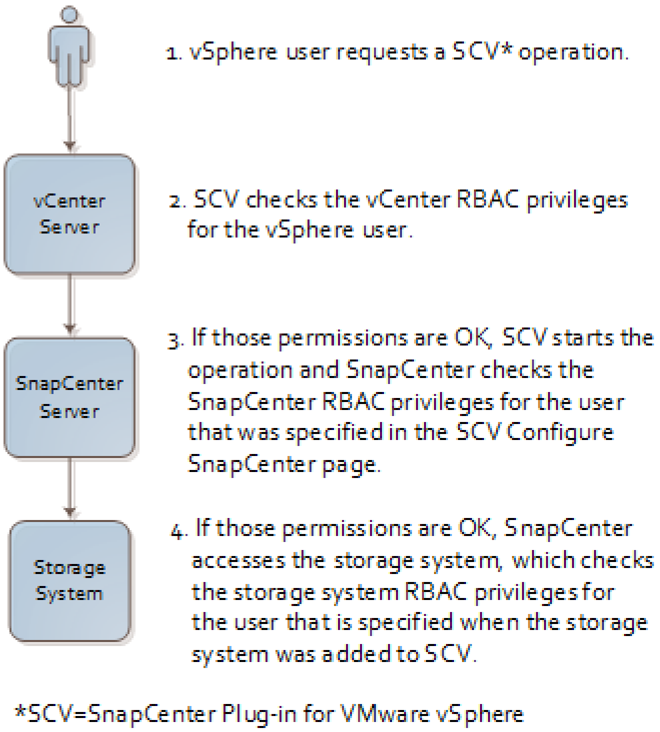
If you are using SnapCenter Plug-in for VMware vSphere, the vCenter Server provides an additional level of RBAC. SnapCenter Plug-in for VMware vSphere supports both vCenter Server RBAC and ONTAP RBAC.

- **vCenter Server RBAC**
  This security mechanism restricts the ability of vSphere users to perform SnapCenter Plug-in for VMware vSphere tasks on vSphere objects, such as virtual machines (VMs) and datastores. The Plug-in for VMware vSphere installation creates roles for SnapCenter operations on vCenter: SCV Administrator, SCV Backup, SCV Guest File Restore, SCV Restore, and SCV View.
  The vSphere administrator sets up vCenter Server RBAC by doing the following:
  - Setting the vCenter Server permissions on the root object (also known as the root folder). You can then refine the security by restricting child entities that do not need those permissions.
  - Assigning the SCV roles to Active Directory users.

  Note: At a minimum, all users must be able to view vCenter objects. Without this privilege, users cannot access the Plug-in for VMware vSphere GUI.

- **ONTAP RBAC**
  This security mechanism restricts the ability of SnapCenter to perform specific storage operations, such as backing up storage for datastores, on a specific storage system.
  ONTAP and SnapCenter RBAC is set up in the following workflow:
  1. The storage administrator creates a role on the SVM with the necessary privileges.
  2. Then the storage administrator assigns the role to a storage user.
  3. The SnapCenter administrator adds the SVM to the SnapCenter Server, using that storage user name.
  4. Then the SnapCenter administrator assigns roles to SnapCenter users.

The following diagram provides an overview of the Plug-in for VMware vSphere validation workflow for RBAC privileges (both vCenter and ONTAP):



1. vSphere user requests a SCV* operation.

2. SCV checks the vCenter RBAC privileges for the vSphere user.

3. If those permissions are OK, SCV starts the operation and SnapCenter checks the SnapCenter RBAC privileges for the user that was specified in the SCV Configure SnapCenter page.

4. If those permissions are OK, SnapCenter accesses the storage system, which checks the storage system RBAC privileges for the user that is specified when the storage system was added to SCV.

*SCV=SnapCenter Plug-in for VMware vSphere

Note: For RBAC to work correctly, you must specify the SnapCenter administrator name as the Domain/Username when you configure the Plug-in for VMware vSphere for the SnapCenter Server.

ONTAP RBAC features in SnapCenter Plug-in for VMware vSphere

ONTAP role-based access control (RBAC) enables you to control access to specific storage systems and the actions a user can perform on those storage systems. SnapCenter Plug-in for VMware vSphere works with vCenter Server RBAC, SnapCenter RBAC, and ONTAP RBAC to determine which SnapCenter tasks a specific user can perform on objects on a specific storage system.

SnapCenter uses the credentials that you set up (user name and password) to authenticate each storage system and determine which operations can be performed on that storage system. The Plug-in for VMware vSphere uses one set of credentials for each storage system. These credentials determine all tasks that can be performed on that storage system; in other words, the credentials are for SnapCenter, not an individual SnapCenter user.

ONTAP RBAC applies only to accessing storage systems and performing SnapCenter tasks related to storage, such as backing up VMs. If you do not have the appropriate ONTAP RBAC privileges for a specific storage system, you cannot perform any tasks on a vSphere object hosted on that storage system.

Each storage system has one set of ONTAP privileges associated with it.

Using both ONTAP RBAC and vCenter Server RBAC provides the following benefits:

- Security
  The administrator can control which users can perform which tasks on both a fine-grained vCenter Server object level and a storage system level.
- Audit information

In many cases, SnapCenter provides an audit trail on the storage system that lets you track events back to the vCenter user who performed the storage modifications.

- Usability
  You can maintain controller credentials in one place.

Product-level privilege required by SnapCenter Plug-in for VMware vSphere

To access the Plug-in for VMware vSphere GUI on vCenter, you must have the product-level, SnapCenter-specific View privilege assigned at the correct vSphere object level. If you log in without this privilege, the Plug-in for VMware vSphere displays an error message when you click the NetApp icon and prevents you from accessing the Plug-in for VMware vSphere GUI.

The following information describes the Plug-in for VMware vSphere product-level View privilege:

Privilege	Description	Assignment level
View	You can access the Plug-in for VMware vSphere GUI. This privilege does not enable you to perform tasks within SnapCenter. To perform any Plug-in for VMware vSphere tasks, you must have the correct SCV-specific and native vCenter Server privileges for those tasks.	The assignment level determines which portions of the UI you can see. Assigning the View privilege at the root object (folder) enables you to enter the Plug-in for VMware vSphere by clicking the NetApp icon. You can assign the View privilege to another vSphere object level; however, doing that limits the the Plug-in for VMware vSphere menus that you can see and use. **Best practice**: The root object is the recommended place to assign any permission containing the View privilege.

Predefined roles packaged with SnapCenter Plug-in for VMware vSphere

To simplify working with vCenter Server RBAC, SnapCenter Plug-in for VMware vSphere provides a set of predefined SnapCenter roles that enable users to perform SnapCenter tasks. There is also a read-only role that allows users to view SnapCenter information, but not perform any tasks.

The predefined Plug-in for VMware vSphere roles have both the required SnapCenter-specific privileges and the native vCenter Server privileges to ensure that tasks complete correctly. In addition, the roles are set up to have the necessary privileges across all supported versions of vCenter Server.

As an administrator, you can assign these roles to the appropriate users.

Note: The Plug-in for VMware vSphere returns these roles to their default values (initial set of privileges) each time you restart the vCenter web client service or modify your installation. If you upgrade the Plug-in for VMware vSphere, the predefined roles are automatically upgraded to work with that version of the plug-in.

You can see the predefined roles in the vCenter GUI by clicking 🏠 > **Administration** > **Roles**.

Role	Description
SCV Administrator	Provides all native vCenter Server and SnapCenter-specific privileges necessary to perform all Plug-in for VMware vSphere tasks.
SCV View	Provides read-only access to all of the Plug-in for VMware vSphere backups, resource groups, and policies.
SCV Backup	Provides all native vCenter Server and SnapCenter-specific privileges necessary to back up vSphere objects (virtual machines and datastores). The user also has access to the configure privilege. The user cannot restore from backups.
SCV Restore	Provides all native vCenter Server and SnapCenter-specific privileges necessary to restore vSphere objects that have been backed up using the Plug-in for VMware vSphere and to restore guest files and folders. The user also has access to the configure privilege. The user cannot back up vSphere objects.
SCV Guest File Restore	Provides all native vCenter Server and SnapCenter-specific privileges necessary to restore guest files and folders. The user cannot restore VMs or VMDKs.

How to configure ONTAP RBAC for SnapCenter Plug-in for VMware vSphere

You must configure ONTAP RBAC on the storage system if you want to use it with SnapCenter Plug-in for VMware vSphere.

From within ONTAP, you must perform the following tasks:

- Create a single role.
  ONTAP 9 Administrator Authentication and RBAC Power Guide
- Create a user name and password (the storage system credentials) in ONTAP for the role.
  This storage system credential is needed to allow you to configure the storage systems for the Plug-in for VMware vSphere. You do this by entering the credentials in the Plug-in for VMware vSphere. Each time you log in to a storage system using these credentials, you are presented with the set of SnapCenter functions that you set up in ONTAP when you created the credentials.

You can use the administrator or root login to access all the SnapCenter tasks; however, it is a good practice to use the RBAC feature provided by ONTAP to create one or more custom accounts with limited access privileges.

Minimum ONTAP privileges required

The minimum ONTAP privileges that are required vary according to the SnapCenter plug-ins you are using for data protection.

All SnapCenter plug-ins require the following minimum privileges, except where noted in the information following these tables.

All-access commands: Minimum privileges required for ONTAP 8.2.*x* and later
`event generate-autosupport-log`

`job history show`
`job stop`

`lun`
`lun create`
`lun delete`
`lun igroup add`
`lun igroup create`
`lun igroup delete`
`lun igroup rename`
`lun igroup show`
`lun mapping add-reporting-nodes`
`lun mapping create`
`lun mapping delete`
`lun mapping remove-reporting-nodes`
`lun mapping show`
`lun modify`
`lun move-in-volume`
`lun offline`
`lun online`
`lun persistent-reservation clear`
`lun resize`
`lun serial`
`lun show`

`snapmirror policy add-rule`
`snapmirror policy modify-rule`
`snapmirror policy remove-rule`
`snapmirror policy show`
`snapmirror restore`
`snapmirror show`
`snapmirror show-history`
`snapmirror update`
`snapmirror update-ls-set`

`version`

All-access commands: Minimum privileges required for ONTAP 8.2.*x* and later

`volume clone create`
`volume clone show`
`volume clone split start`
`volume clone split stop`
`volume create`
`volume destroy`
`volume file clone create`
`volume file show-disk-usage`
`volume offline`
`volume online`
`volume modify`
`volume qtree create`
`volume qtree delete`
`volume qtree modify`
`volume qtree show`
`volume restrict`
`volume show`
`volume snapshot create`
`volume snapshot delete`
`volume snapshot modify`
`volume snapshot rename`
`volume snapshot restore`
`volume snapshot restore-file`
`volume snapshot show`
`volume unmount`

`vserver cifs`
`vserver cifs share create`
`vserver cifs share delete`
`vserver cifs shadowcopy show`
`vserver cifs share show`
`vserver cifs show`
`vserver export-policy`
`vserver export-policy create`
`vserver export-policy delete`
`vserver export-policy rule create`
`vserver export-policy rule show`
`vserver export-policy show`
`vserver iscsi`
`vserver iscsi connection show`
`vserver show`

Read-only commands: Minimum privileges required for ONTAP 8.2.*x* and later
`network interface`
`network interface show`
`vserver`

Additional information for SnapCenter Plug-in for Microsoft SQL Server

- All-access command privilege that is not required: `lun persistent-reservation clear`.
- If you are protecting virtualized databases or databases on VMs, you must also comply with the requirements for SnapCenter Plug-in for VMware vSphere.

Additional information for SnapCenter Plug-in for Oracle Database

- All-access command privileges that are not required:

  ```
  vserver cifs share create
  vserver cifs share delete
  vserver cifs share show
  vserver cifs show
  vserver export-policy
  vserver export-policy create
  vserver export-policy delete
  vserver export-policy rule create
  vserver export-policy rule show
  vserver export-policy show
  vserver iscsi
  vserver iscsi connection show
  ```

- Read-only command privileges that are not required:

  ```
  network interface
  network interface show
  vserver
  ```

- Additional all-access command privileges that are required:

  ```
  lun attribute show
  lun geometry
  network interface
  network interface show
  vserver
  ```

- If you are protecting virtualized databases or databases on VMs, you must also comply with the requirements for SnapCenter Plug-in for VMware vSphere.

Additional information for SnapCenter Plug-in for Microsoft Windows

- All-access command privilege that is not required: `lun persistent-reservation clear`.
- If you are protecting virtualized file systems or file systems on VMs, you must also comply with the requirements for SnapCenter Plug-in for VMware vSphere.

Additional information for SnapCenter Plug-in for VMware vSphere

- If you are running ONTAP 8.2.*x*
  You must login as `vsadmin` on the SVM to have the appropriate privileges for SnapCenter Plug-in for VMware vSphere operations.

- If you are running ONTAP 8.3 and later
  You must login as `vsadmin` or with a role that has the minimum privileges listed in the tables in this appendix.

Additional information for SnapCenter Custom Plug-ins

- All-access command privileges that are not required:

  ```
  lun
  lun persistent-reservation clear
  vserver export-policy
  vserver iscsi
  ```

- Read-only command privileges that are not required:

  ```
  network interface show
  vserver
  ```

- Additional all-access command privileges that are required:

  ```
  lun attribute show
  lun geometry
  network interface
  vserver cifs shadowcopy show
  ```

- If you are protecting virtualized data or data on VMs, you must also comply with the requirements for SnapCenter Plug-in for VMware vSphere.

Backing up VMs, VMDKs, and datastores

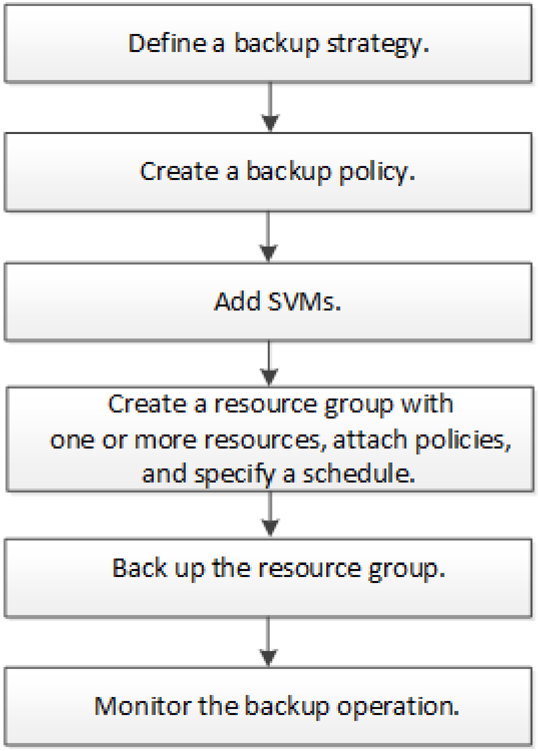
The SnapCenter Plug-in for VMware vSphere web client performs data protection operations for VMs, VMDKs, and datastores. All backup operations are performed on resource groups, which can contain any combination of one or more VMs and datastores. You can back up on demand or according to a defined protection schedule.

When you back up a datastore, you are backing up all the VMs in that datastore.

Note: The Plug-in for VMware vSphere does not support backing up datastore clusters directly. However, you can put all the datastores that belong to a datastore cluster into a resource group and back up that resource group.

Backup and restore operations cannot be performed simultaneously on the same resource.

The following workflow shows the sequence in which you must perform the backup operations:


Define a backup strategy.
Create a backup policy.
Add SVMs.
Create a resource group with one or more resources, attach policies, and specify a schedule.
Back up the resource group.
Monitor the backup operation.

Note: SnapCenter backs up SAN and NAS datastores; it does not back up VSAN or VVOL datastores.

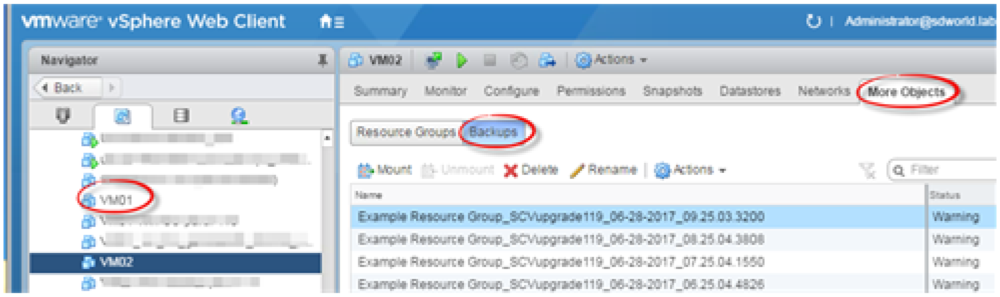
Note: If a VM contains a database, then backing up the VM is not the same as backing up the database; it does not provide an application-consistent backup. To perform an application-consistent back up of a database, you must use one of the SnapCenter database plug-ins.

Viewing VM and datastore backups

When you are preparing to back up or restore a resource, you might want to see all the backups that are available for that resource and view details of those backups.

Steps

1. In the VMware vSphere web client in vCenter, click in the toolbar, and then select **VMs and Templates** from the drop-down list.
2. In the left Navigator pane, select a VM for which you want to view backups, then select the **Related Objects** tab (or **More Objects** in vCenter 6.5), and then select the **Backups** tab.



Name	Status
Example Resource Group_SCVupgrade119_06-28-2017_09.25.03.3200	Warning
Example Resource Group_SCVupgrade119_06-28-2017_08.25.04.3808	Warning
Example Resource Group_SCVupgrade119_06-28-2017_07.25.04.1550	Warning
Example Resource Group_SCVupgrade119_06-28-2017_06.25.04.4826	Warning

3. Double-click the backup that you want to view.

Adding SVMs using the VMware vSphere web client GUI

Before you can backup or restore VMs, you must add the SVMs on which the VMs are located. Adding SVMs enables SnapCenter to recognize and manage backup and restore operations.

About this task

When SnapCenter Plug-in for VMware vSphere adds an SVM to vCenter, it also provides that information to SnapCenter Server. You can also use the SnapCenter GUI to perform the same operations.

> **Note:** SnapCenter only performs backup and restore operations on directly-connected SVMs. It does not operate at the cluster management LIF level.

Steps

1. In the left Navigator pane of the VMware vSphere web client in vCenter for the Plug-in for VMware vSphere, click **Storage Systems**.
2. On the **Storage Systems** page, click **Add Storage System**.
3. In the **Add Storage System** dialog box, enter the SVM information:

For this field…	Do this…
vCenter Server	Select the vCenter Server.
Storage system	Enter the name or SVM FQDN or IP address.
User name	Enter the user name that is used to log on to the SVM. For example, you might enter the ONTAP user name.

For this field…	Do this…
Password	Enter the SVM log on password.
Protocol	Select HTTP or HTTPS.
Port	Enter the SVM port used to communicate with vCenter. The default port is 443.
Timeout	Enter the number of seconds vCenter waits before timing out the operation. The default is 60 seconds.

4. Check the **Enable Autosupport on failure** box if you want Autosupport notification for failed data protection jobs.

   You must also enable Autosupport on the SVM and configure the Autosupport email settings.

5. Click **Add**.

Creating backup policies for VMs and datastores

You must create backup policies before you use SnapCenter Plug-in for VMware vSphere to back up VMs and datastores.

Before you begin

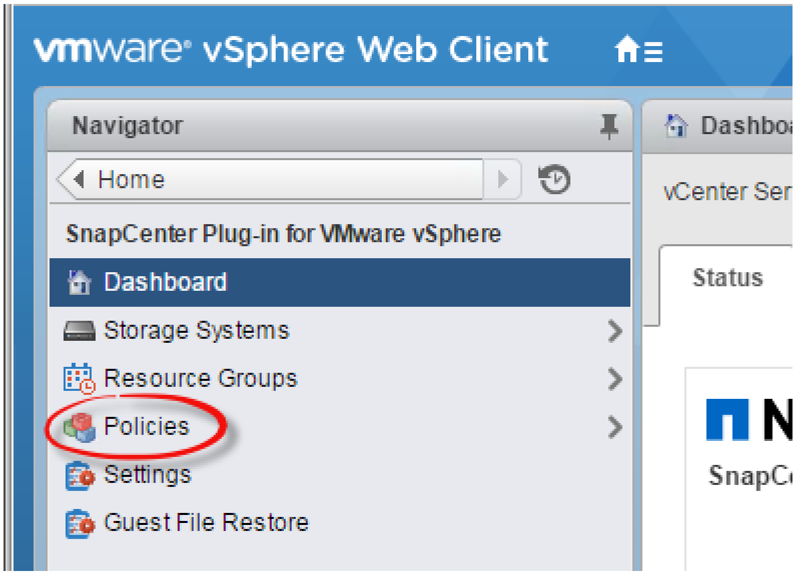
- You must have defined your backup strategy.
  For details, see the information about defining a data protection strategy for VMs and datastores.
  SnapCenter concepts
- You must have read the prerequisites.
- You must have secondary storage relationships configured.
  If you are replicating Snapshot copies to a mirror or vault secondary storage, the relationships must be configured and the SnapCenter administrator must have assigned the SVMs to you for both the source and destination volumes.
  For information about how administrators assign resources to users, see the SnapCenter installation information.

About this task

Most of the fields on these wizard pages are self-explanatory. The following information describes some of the fields for which you might require guidance.

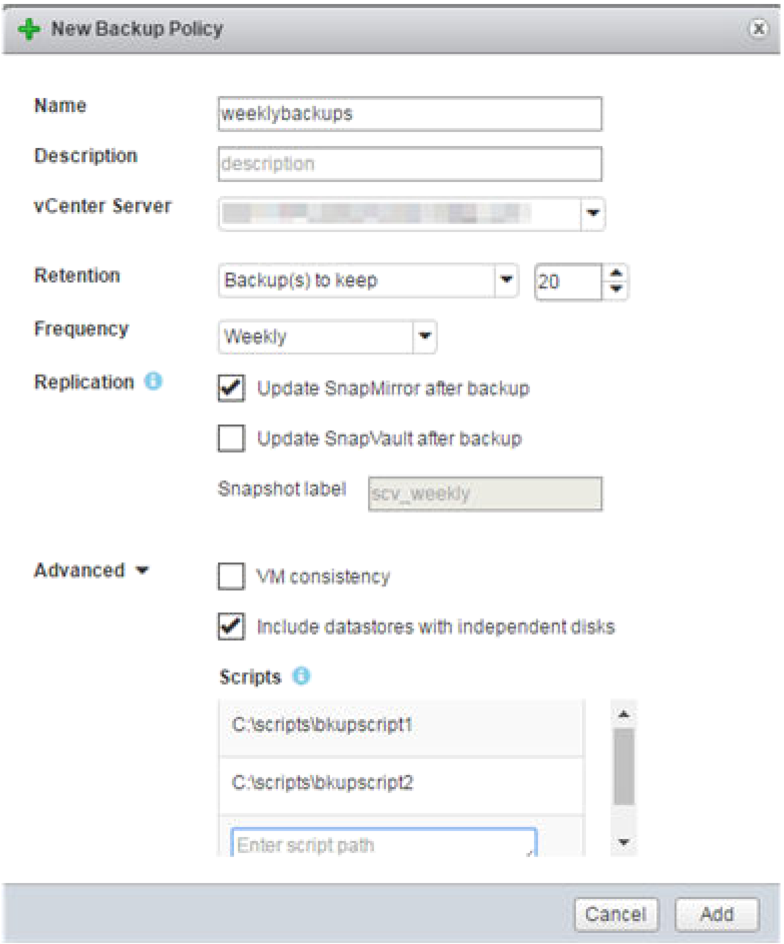
Steps

1. In the left Navigator pane of the VMware vSphere web client in vCenter for the Plug-in for VMware vSphere, click **Policies**.



2. In the **Policies** page, click **New Policy** in the toolbar.

3. In the **New Backup Policy** page, enter the policy name and a description.



Name: weeklybackups
Description: description
vCenter Server:
Retention: Backup(s) to keep 20
Frequency: Weekly
Replication: ☑ Update SnapMirror after backup
☐ Update SnapVault after backup
Snapshot label: scv_weekly
☐ VM consistency
☑ Include datastores with independent disks
C:\scripts\bkupscript1
C:\scripts\bkupscript2

- Supported characters
  Do not use the following special characters in VM, datastore, policy, backup, or resource group names: % & * $ # @ ! \ / : * ? " < > - | ; ' , .
  An underscore character (_) is allowed.

- Server address
  The wizard automatically enters the vCenter Server address.

4. Specify the retention settings.

> **Important:** You should set the retention count to 2 or higher if you plan to enable SnapVault replication. If you set the replication count to 1, the retention operation can fail. This is because the first Snapshot copy is the reference Snapshot copy for the SnapVault relationship until the newer Snapshot copy is replicated to the target.

5. Specify the frequency settings.

The policy specifies the backup frequency only. The specific protection schedule for backing up is defined in the resource group. Therefore, two or more resource groups can share the same policy and backup frequency but have different backup schedules.

6. In the **Replication** fields, specify replication to secondary storage:

For this field…	Do this…
Update SnapMirror after backup	Select this option to create mirror copies of backup sets on another volume that has a SnapMirror relationship to the primary backup volume. If a volume is configured with a policy type that specifies a mirror-vault relationship, and this option is selected, then the backup is also copied to any vault destination.
Update SnapVault after backup	Select this option to perform disk-to-disk backup replication on another volume that has a SnapVault relationship to the primary backup volume. **Note:** A maximum of 31 characters is allowed for SnapVault labels.
Snapshot label	Enter an optional, custom label to be added to SnapVault Snapshot copies created with this policy. The Snapshot label helps to distinguish Snapshots created with this policy from other Snapshots on the secondary storage system. **Note:** Custom Snapshot copy labels are supported only for SnapVault labels; not for SnapMirror or backup copies.

7. Optional: In the **Advanced** fields, select the fields that are needed.

For this field…	Do this…
VM consistency	Check this box to quiesce the VMs and create a VMware snapshot each time the backup job runs. **Note:** When you check the VM consistency box, backup operations might take longer and require more storage space. In this scenario, the VMs are first quiesced, then VMware performs a crash consistent snapshot, then SnapCenter performs its backup operation, and then VM operations are resumed.
Include datastores with independent disks	Check this box to include in the backup any datastores with independent disks that contain temporary data.

For this field…	Do this…
Scripts	Enter the fully qualified path of the prescript or postscript that you want the Plug-in for VMware vSphere to run before or after backup operations. For example, you can run a script to update SNMP traps, automate alerts, and send logs. **Note:** Prescripts and postscripts must be located on the SnapCenter Server. Therefore, the path you specify must reflect that location. To enter multiple scripts, press **Enter** after each script path to list each script on a separate line. The character ";" is not allowed.

8. Click **Finish**.

You can verify that the policy is created and review the policy configuration by selecting the policy in the Policies page.

Related information

Installing and setting up SnapCenter
Performing administrative tasks with SnapCenter

Prescripts and postscripts

You can use custom prescripts and postscripts as part of your data protection operations. These scripts enable automation either before your data protection job or after. For example, you might include a script that automatically notifies you of data protection job failures or warnings. Before you set up your prescripts and postscripts, you should understand some of the requirements for creating these scripts.

Supported script types

The following type of scripts are supported:

- Batch files
- PowerShell scripts
- Perl scripts

Script path location

All prescripts and postscripts that are run as part of SnapCenter operations, on nonvirtualized and on virtualized storage systems, are executed on the SnapCenter Server. Therefore, the scripts must be located on the SnapCenter Server and the path you specify must reflect that location. If the SnapCenter Server host is in a HA configuration, you must specify a script that is accessible from both NLB nodes.

Where to specify scripts

Scripts are specified in backup policies. When a backup job is started, the policy automatically associates the script with the resources being backed up.

When you create a backup policy, the wizards in some plug-ins provide separate fields to specify prescripts and postscripts. Other wizards only provide a single field for both.

To specify multiple scripts, press **Enter** after each script path to list each script on a separate line. Semicolons (;) are not allowed. You can specify multiple prescripts and multiple postscripts. A single script can be coded as both a prescript and a postscript and can call other scripts.

When scripts are executed

Scripts are executed according to the value set for `BACKUP_PHASE`.

- `BACKUP_PHASE=PRE_BACKUP`
  Prescripts are executed in the `PRE_BACKUP` phase of the operation.

  Note: If a prescript fails, the backup also fails.

- `BACKUP_PHASE=POST_BACKUP` or `BACKUP_PHASE=FAILED_BACKUP`
  Postscripts are executed in the `POST_BACKUP` phase of the operation after the backup completes successfully or in the `FAILED_BACKUP` phase if the backup does not complete successfully.

  Note: If a postscript fails, the backup completes successfully and a warning message is sent.

Environment variables passed to scripts

You can use the following environment variables in scripts.

Environment variable	Description
`BACKUP_NAME`	Name of the backup. Variable passed in postscripts only.
`BACKUP_DATE`	Date of the backup, in the format *`yyyymmdd`* Variable passed in postscripts only.
`BACKUP_TIME`	Time of the backup, in the format *`hhmmss`* Variable passed in postscripts only.
`BACKUP_PHASE`	The phase of the backup in which you want the script to run. Valid values are: `PRE_BACKUP`, `POST_BACKUP`, and `FAILED_BACKUP`. Variable passed in prescripts and postscripts.
`STORAGE_SNAPSHOTS`	The number of storage snapshots in the backup. Variable passed in postscripts only.
`STORAGE_SNAPSHOT.#`	One of the defined storage snapshots, in the following format: `<filer>:/vol /<volume>:<ONTAP-snapshot-name>` Variable passed in postscripts only.
`VIRTUAL_MACHINES`	The number of VMs in the backup. Variable passed in prescripts and postscripts.

<table>
<tr><th>Environment variable</th><th>Description</th></tr>
<tr><td><code>VIRTUAL_MACHINE.#</code></td><td>One of the defined virtual machines, in the following format:<pre><em><VM name>|<VM UUID>|
<power-state>|<VM snapshot>|
<ip-addresses></em></pre><em><code>power-state</code></em> has the values <code>POWERED_ON</code>, <code>POWERED_OFF</code>, or <code>SUSPENDED</code>
<em><code>VM snapshot</code></em> has the values <code>true</code> or <code>false</code>
Variable passed in prescripts and postscripts.</td></tr>
</table>

Script timeouts

The timeout for backup scripts is 15 minutes and cannot be modified.

Creating resource groups for VMs and datastores

A resource group is the container to which you add one or more VMs and datastores that you want to protect; called a *backup job* in Virtual Storage Console (VSC). For example, you can simultaneously back up all the VMs that are associated with a given application, or you can back up a single VM, or you can back up all the VMs in a datastore. Resource groups can contain any combination of VMs and datastores.

About this task

You can add or remove VMs and datastores from a resource group at any time.

Note: A resource group can contain VMs, and SAN and NAS datastores; it cannot contain VSAN or VVOL datastores.

- Backing up a single resource
  To back up a single resource, you must create a resource group that contains that single resource.
- Backing up multiple resources
  To back up multiple resources, you must create a resource group that contains multiple resources.
- Optimizing Snapshot copies
  To optimize Snapshot copies, you should group into one resource group the VMs and datastores that are associated with the same volume.
- Backup policies
  Although it is possible to create a resource group without a backup policy, you can only perform data protection operations when at least one policy is attached to the resource group. You can use an existing policy or you can create a new policy while creating a resource group.

Steps

1. In the left Navigator pane of the VMware vSphere web client in vCenter for the Plug-in for VMware vSphere, click **Resource Groups** and then click ➕ (Create Resource Group).

   This is the easiest way to create a resource group. However, you can also create a resource group with one resource by performing one of the following:

- To create a resource group for one VM, click 🏠 > **VMs and Templates** then right-click a VM, select **NetApp SnapCenter** from the drop-down list, and then select **Create Resource Group** from the secondary drop-down list.

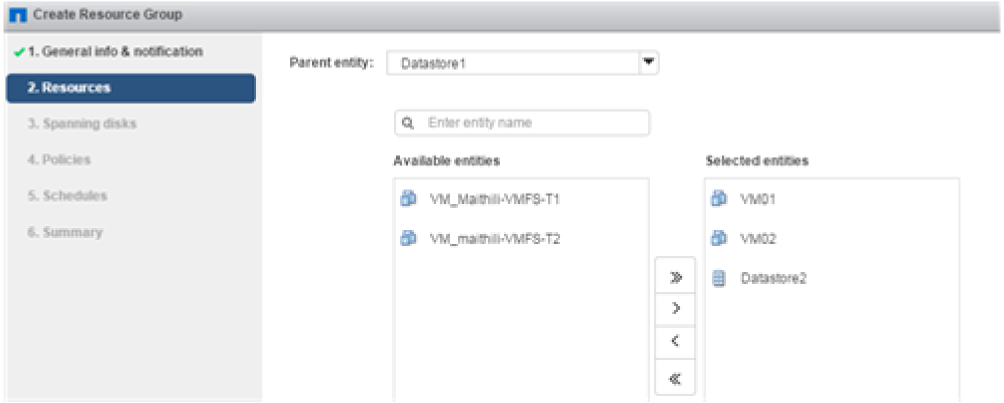
- To create a resource group for one datastore, click 🏠 > **Storage** then right-click a datastore, select **NetApp SnapCenter** from the drop-down list, and then select **Create Resource Group** from the secondary drop-down list.

The Create Resource Group wizard begins.

2. In the **General Info & Notification** page in the wizard, do the following:

For this field…	Do this…
Name	Enter a name for the resource group. Do not use the following special characters in VM, datastore, policy, baqckup, or resource group names: % & * $ # @ ! \ / : * ? " < > - | ; ' , . An underscore character (_) is allowed. VM or datastore names with special characters are truncated, which makes it difficult to search for a specific backup.
Description	Enter a description of the resource group.
Notification	From the drop-down list, select when you want to receive notifications about operations on this resource group: Error or warnings: Send notification for errors and warnings only Errors: Send notification for errors only Always: Send notification for all message types Never: Do not send notification
Email send from	Enter the email address you want the notification sent from.
Email send to	Enter the email address of the person you want to receive the notification. For multiple recipients, use a comma to separate the email addresses.
Email subject	Enter the subject you want for the notification emails.

3. On the **Resources** page, in the Available Entities list, select the resources you want in the resource group, then click > to move your selections to the Selected Resources list.



Parent entity: Datastore1

By default, the Available Entities list displays the Datacenter object and the selection options display the datastores. You can click a datastore to view the VMs within the datastore and add them to the resource group.

When you click **Next**, the system first checks that SnapCenter manages and is compatible with the storage on which the selected VMs or datastores are located.

If the message `Some entities are not SnapCenter compatible` is displayed, then a selected VM or datastore is not compatible with SnapCenter. See the Troubleshooting section for more information.

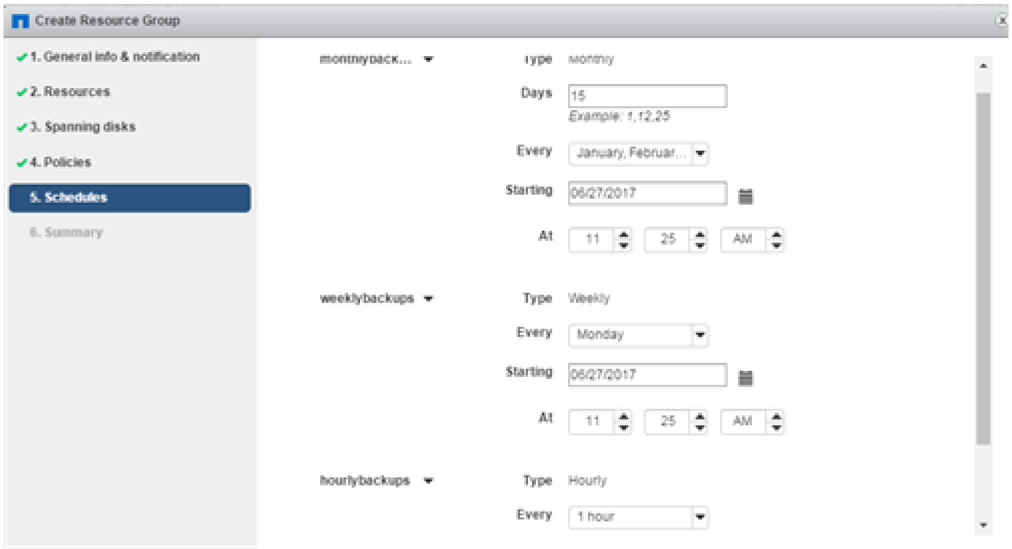
4. On the **Spanning Disks** page, select an option for VMs with multiple VMDKs across multiple datastores:

   Always exclude all spanning datastores [This is the default for datastores.]
   Always include all spanning datastores [This is the default for VMs.]
   Manually select the spanning datastores to be included

5. On the **Policies** page, select one or more policies from the list.

To use...	Do this...
An existing policy	Select one or more policies from the list.
A new policy	**a.** Click ✚ **Create Policy**. **b.** Complete the New Backup Policy wizard to return to the Create Resource Group wizard.

6. On the **Schedules** page, configure the backup schedule for each selected policy.



monthlyback...
Type: Monthly
Days: 15
Example: 1,12,25
Every: January, Februar...
Starting: 06/27/2017
At: 11 25 AM

weeklybackups
Type: Weekly
Every: Monday
Starting: 06/27/2017
At: 11 25 AM

hourlybackups
Type: Hourly
Every: 1 hour

You must fill in each field.

7. Review the summary, and then click **Finish**.

   Before you click **Finish**, you can go back to any page in the wizard and change the information.

   After you click **Finish**, the new resource group is added to the resource groups list.

Related tasks

Creating backup policies for VMs and datastores on page 26
Adding a single VM or datastore to a resource group on page 34

Related references

SnapCenter compatibility check fails on page 74

Adding a single VM or datastore to a resource group

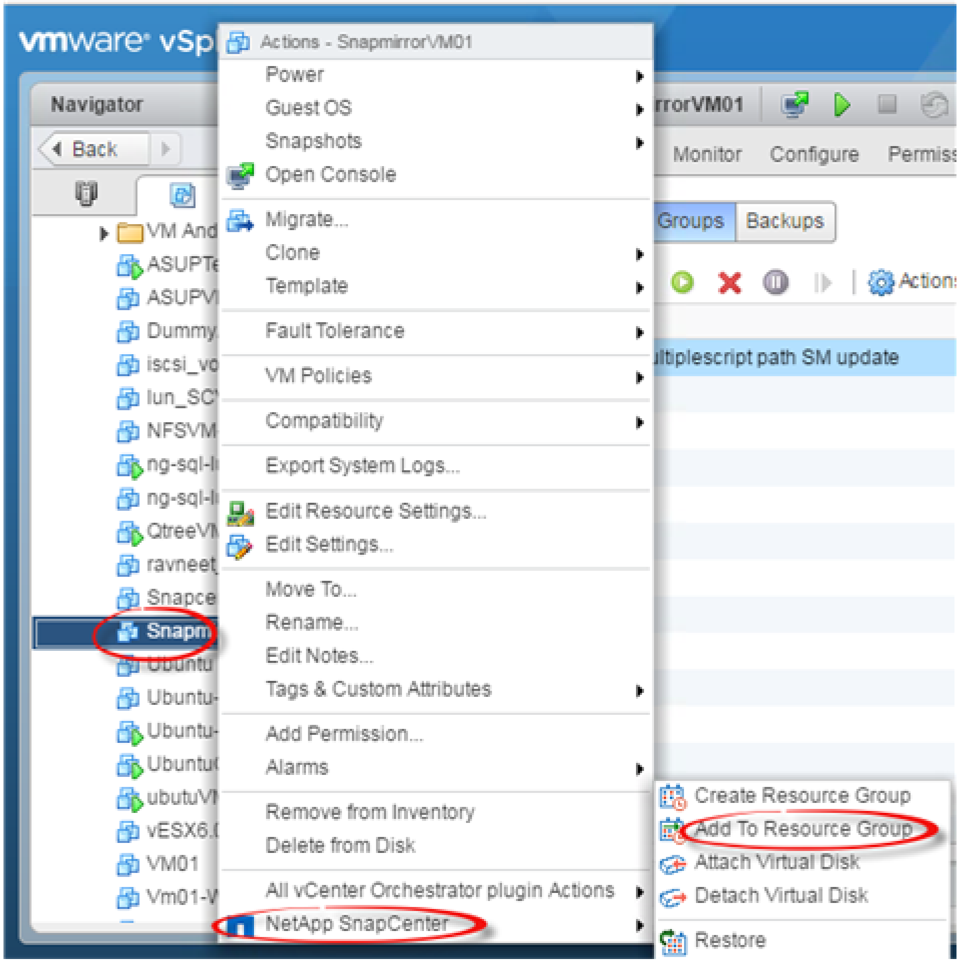
You can quickly add a single VM or datastore to any existing resource group managed by the Plug-in for VMware vSphere.

About this task

You can add SAN and NAS datastores but not VSAN or VVOL datastores.

Steps

1. In the VMware vSphere web client GUI, click in the toolbar, and navigate to the VM or datastore that you want to add.
2. In the left Navigator pane, right-click on the VM or datastore, select **NetApp SnapCenter** from the drop-down list, and then select **Add To Resource Group** from the secondary drop-down list.



The system first checks that SnapCenter manages and is compatible with the storage on which the selected VM is located and then displays the Add To Resource Group page. If the message `SnapCenter Compatibility Error` is displayed, then the selected VM is not compatible with SnapCenter. If the selected VM is not compatible, then you must first add the appropriate SVM to SnapCenter.

3. In the **Add To Resource Group** page, select a resource group, and then click **OK**.

Related tasks

Adding SVMs using the VMware vSphere web client GUI on page 25

Adding multiple VMs and datastores to a resource group

You can add multiple VMs and datastores to any existing resource group by using the Plug-in for VMware vSphere Edit Resource Group wizard.

About this task

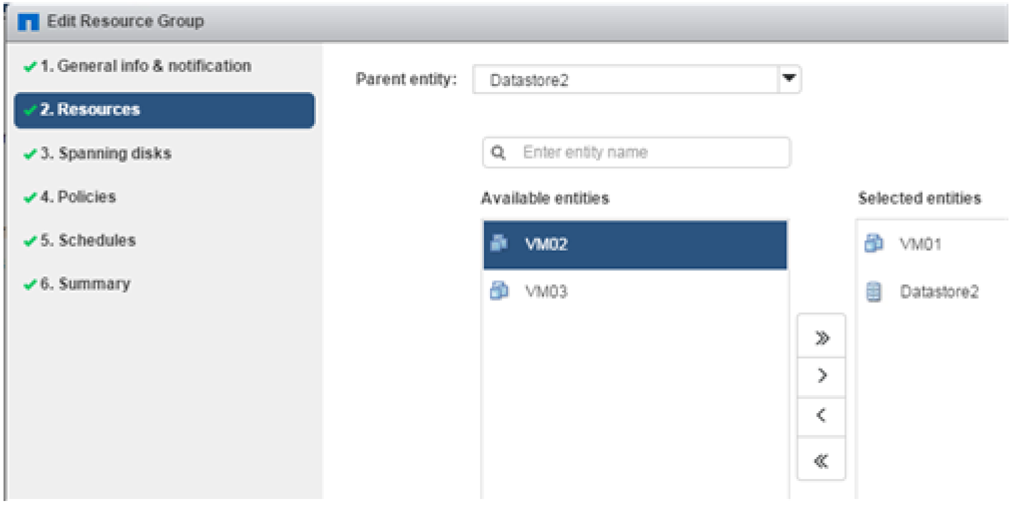
Note: You can add SAN and NAS datastores but not VSAN or VVOL datastores.

Steps

1. In the left Navigator pane of the VMware vSphere web client in vCenter for the Plug-in for VMware vSphere, click **Resource Groups**, then select a resource group, and then click ✏ (Edit).

   The Edit Resource Group wizard begins.

2. On the **Resources** page, in the Available Entities list, select a VM or datastore you want to add to the resource group, then click > to move your selection to the Selected Resources list. You can move all the available entities by clicking >>.

   Parent entity: Datastore2

   By default, the Available Entities list displays the Datacenter object. You can click a datastore to view the VMs within the datastore and add them to the resource group.

   When you click **Next**, the system first checks that SnapCenter manages and is compatible with the storage on which the selected VMs or datastores are located. If the message `SnapCenter Compatibility Error` is displayed, then a selected VM or datastore is not compatible with SnapCenter.

3. Repeat Step 2 for each VM or datastore that you want to add.

4. Click **Next** until you reach the **Summary** page, and then review the summary and click **Finish**.

Backing up VM and datastore resource groups on demand

A backup operation on a resource group is performed on all the resources defined in the resource group. You can back up a resource group on demand from the VMware vSphere web client GUI in vCenter. If a resource group has a policy attached and a schedule configured, then backups occur automatically according to the schedule.

Before you begin

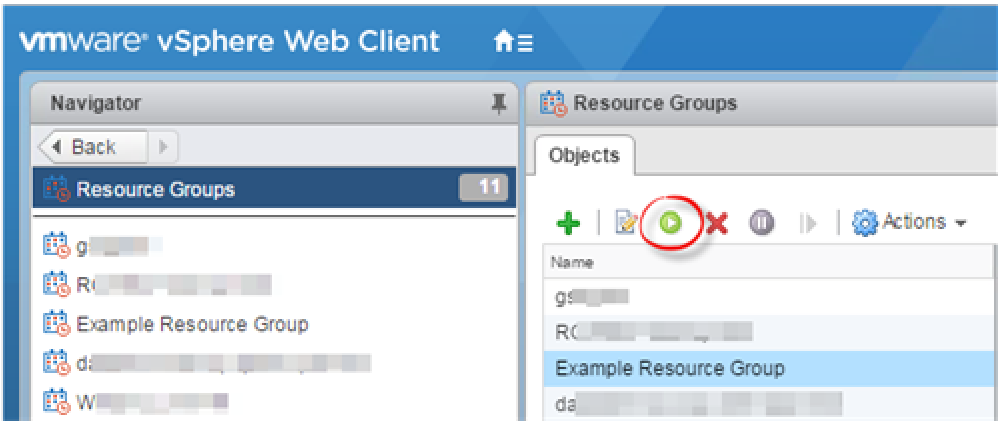
- You must have created a resource group with a policy attached.
- If you are backing up a resource that has a SnapMirror relationship to secondary storage, you must have SnapCenter admin privileges.

About this task

Note: In Virtual Storage Console (VSC), you could perform an on-demand backup without having a *backup job* configured for a VM or datastore. However, in SnapCenter Plug-in for VMware vSphere, VMs and datastores must be in a resource group before you can perform backups.

Steps

1. In the VMware vSphere web client in vCenter, click ⌂ in the toolbar, and then select **SnapCenter Plug-in for VMware** from the drop-down list.
2. In the left Navigator pane, click **Resource Groups**.
3. In the **Objects** tab of the **Resource Groups** page, select the resource group you want to back up, and then click ▶ (Run Now) in the toolbar.



4. If the resource group has multiple policies configured, then in the **Backup Now** dialog box, select from the drop-down list the policy you want to use for this backup operation, and then click **Yes**.
5. Click **OK** to start the backup.
6. Optional: Monitor the operation progress by clicking **Recent Tasks** at the bottom of the window or on the dashboard **Job Monitor** for more detail.

Related tasks

Creating backup policies for VMs and datastores on page 26
Creating resource groups for VMs and datastores on page 31
Viewing VM and datastore backups on page 25

Restoring VMs, VMDKs, files, and folders from backups

You can restore VMs and VMDKs from primary or secondary backups. VMs are always restored to the original host and datastore; VMDKs can be restored to either the original or an alternate datastore. You cannot use SnapCenter Plug-in for VMware vSphere to restore a datastore, only the individual VMs in the datastore. You can also restore individual files and folders in a guest file restore session, which attaches a backup copy of a virtual disk and then restores the selected files or folders.

Related tasks

Searching for backups on page 38
Attaching VMDKs to a VM on page 50
Restoring VMs from backups on page 39

How restore operations are performed

For VMFS environments, the Plug-in for VMware vSphere uses clone and mount operations with Storage VMotion to perform restore operations. For NFS environments, the Plug-in for VMware vSphere uses native ONTAP Single File SnapRestore (SFSR) to provide greater efficiency for most restore operations.

Restore operations	**NFS environments**		**VMFS environments**
	Performed using ONTAP SFSR	**Performed using clone and mount with Storage VMotion**	**Performed using clone and mount with Storage VMotion**
Restoring VMs and VMDKs from primary backups	✓		✓
Restoring VMs and VMDKs from secondary backups	✓		✓
Restoring deleted VMs and VMDKs from primary backups	✓		✓
Restoring deleted VMs and VMDKs from secondary backups		✓	✓
Restoring VMs and VMDKs from VM-consistent primary backups	✓		✓
Restoring VMs and VMDKs from VM-consistent secondary backups		✓	✓

Guest file restore operations are performed using clone and mount operations (not Storage VMotion) in both NFS and VMFS environments.

Searching for backups

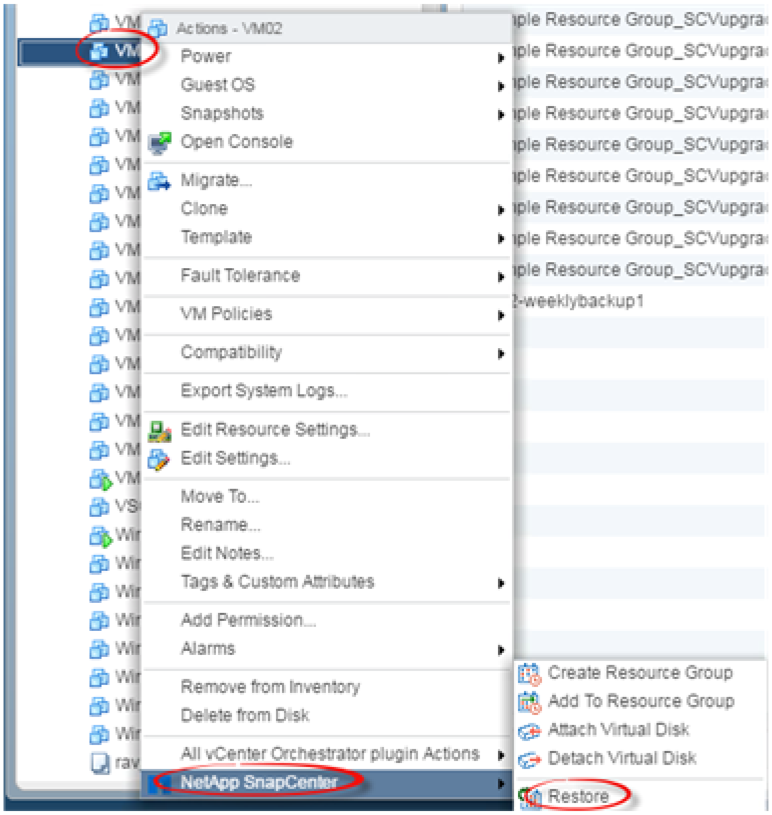
You can search for and find a specific backup of a VM or datastore using the Restore wizard. After you locate a backup, you can then restore it.

Steps

1. In the VMware vSphere web client GUI, click in the toolbar, and then do one of the following:

To view backups for...	Do the following...
VMs	Select **VMs and Templates** from the drop-down list.
Datastores	Select **Storage** from the drop-down list.

2. In the left Navigator pane, expand the datacenter that contains the VM or datastore.
3. Optional: Right-click a VM or datastore, then select **NetApp SnapCenter** in the drop-down list, and then select **Restore** in the secondary drop-down list.



4. In the **Restore** wizard enter a search name and click **Search**.

   You can filter the backup list by clicking (filter icon) and selecting a date and time range, selecting whether you want backups that contain VMware Snapshots, whether you want mounted backups, and the location. Click **OK**.

Restoring VMs from backups

When you restore a VM, you overwrite the existing content with the backup copy that you select. You can restore VMs from either a primary or secondary backup to the same ESXi server.

Before you begin

A backup must exist. You must have created a backup of the VM using SnapCenter Plug-in for VMware vSphere before you can restore the VM.

About this task

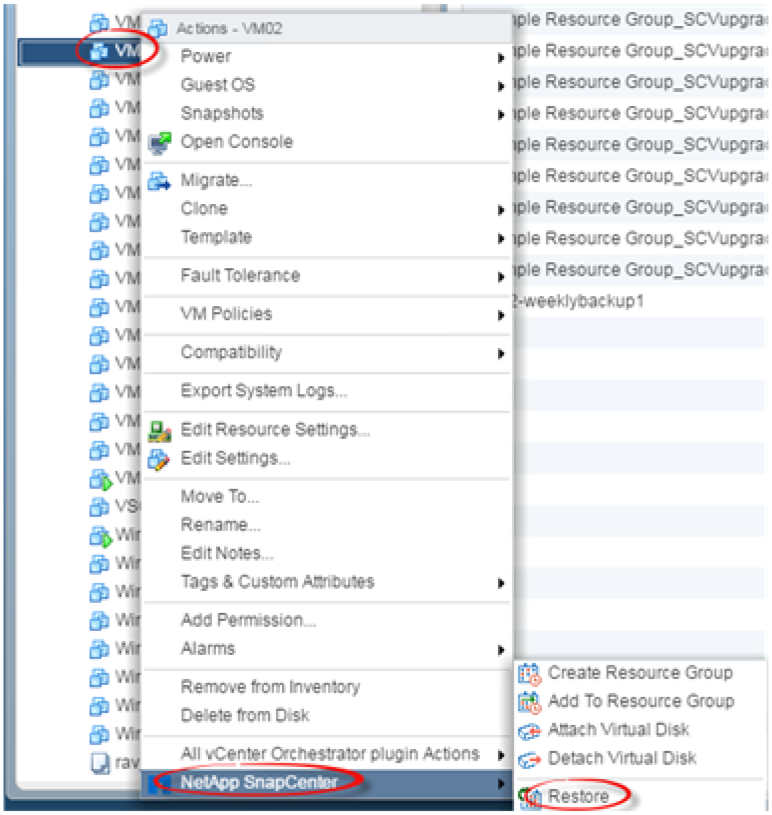
- VM is unregistered and registered again
  The restore operation for VMs unregisters the original VM, restores the VM from a backup Snapshot copy, and registers the restored VM with the same name and configuration on the same ESXi server.
- Restoring datastores
  You cannot restore a datastore, but you can restore any VM in the datastore.
- VMware consistency snapshot failures for a VM
  Even if a VMware consistency snapshot for a VM fails, the VM is nevertheless backed up. You can view the entities contained in the backup copy in the Restore wizard and use it for restore operations.
- A restore operation might fail if the storage tier of the FabricPool where the VM is located is unavailable.

Steps

1. In the VMware vSphere web client GUI, click 🏠 in the toolbar, and then select **VMs and Templates** from the drop-down list.

   Note: If you are restoring a deleted VM, you must log on with `vsadmin` or a user account that has all the same privileges as `vsadmin`. The host must be on a storage system that is running ONTAP 8.2.2 or later.

2. In the left Navigator pane, right-click a VM, then select **NetApp SnapCenter** in the drop-down list, and then select **Restore** in the secondary drop-down list.



3. In the **Restore** wizard, on the **Select Backup** page, select the backup copy that you want to restore from.

   You can search for a specific backup name or a partial backup name, or you can filter the backup list by clicking (filter icon) and selecting a date and time range, selecting whether you want backups that contain VMware Snapshots, whether you want mounted back ups, and the location. Click **OK** to return to the wizard.

4. On the **Select Scope** page, click **Entire virtual machine** in the **Restore scope** field and then select the ESXi host where the backup should be mounted.

   The restore destination is the same ESXi host where the VM was originally registered.

5. On the **Select Location** page, select the location of the datastore that you want to restore from.

6. Review the Summary page and then click **Finish**.

7. Optional: Monitor the operation progress by clicking **Recent Tasks** at the bottom of the screen.

   Refresh the screen to display updated information.

Related concepts

How restore operations are performed on page 37

Restoring deleted VMs from backups

You can restore a deleted VM from a datastore primary or secondary backup to an ESXi host that you select.

Before you begin

- The user account for the storage system on the Storage Systems page in the SnapCenter Plug-in for VMware vSphere GUI in vCenter, must have the minimum ONTAP privileges required for ONTAP operations, as listed in the concepts and installation information.
  SnapCenter concepts
  Installing and setting up SnapCenter
- A backup must exist.
  You must have created a backup of the VM using SnapCenter Plug-in for VMware vSphere before you can restore the VMDKs on that VM.

About this task

You cannot restore a datastore, but you can restore any VM in the datastore.

Note: A restore operation might fail if the storage tier of the FabricPool where the VM is located is unavailable.

Steps

1. In the VMware vSphere web client GUI, click 🏠 in the toolbar, and then select **Storage** from the drop-down list.
2. Select the datastore on which the deleted VM was located, then select the **Related Objects** tab (or **More Objects** tab in vCenter 6.5), and then select the **Backups** tab.
3. Double-click on a backup to see a list of all VMs that are included in the backup.
4. Select the deleted VM from the backup list and then click **Restore**.
5. In the **Restore** wizard, on the **Select Backup** page, select the backup copy that you want to restore from.

   You can search for a specific backup name or a partial backup name, or you can filter the backup list by clicking (filter icon) and selecting a date and time range, selecting whether you want backups that contain VMware Snapshots, whether you want mounted back ups, and the location. Click **OK** to return to the wizard.
6. On the **Select Scope** page, click **Entire virtual machine** in the **Restore scope** field and then select the Destination ESXi host name.

   The restore destination can be any ESXi host that has been added to SnapCenter. This option restores the contents of the last datastore in which the VM resided from a Snapshot copy with the specified time and date. The **Restart VM** check box is checked if you select this option.

   If you are restoring a VM in an NFS datastore onto an alternate ESXi host that is in an ESXi cluster, then after the VM is restored, it is registered on the alternate host.
7. On the **Select Location** page, select the location of the datastore that you want to restore from.
8. Review the Summary page and then click **Finish**.

9. Optional: Monitor the operation progress by clicking **Recent Tasks** at the bottom of the screen.

   Refresh the screen to display updated information.

Related concepts

How restore operations are performed on page 37

Restoring VMDKs from backups

You can restore one or more virtual machine disks (VMDKs) on a VM to the same ESXi server or to an alternate one. You can restore existing VMDKs, or deleted or detached VMDKs from either a primary a secondary backup. If restoring to the same host, you overwrite the existing content with the backup copy.

Before you begin

- The user account for the storage system on the Storage Systems page in the SnapCenter Plug-in for VMware vSphere GUI in vCenter, must have the minimum ONTAP privileges required for ONTAP operations, as listed in the concepts and installation information.
  SnapCenter concepts
  Installing and setting up SnapCenter
- A backup must exist.
  You must have created a backup of the VM using SnapCenter Plug-in for VMware vSphere before you can restore the VMDKs on that VM.

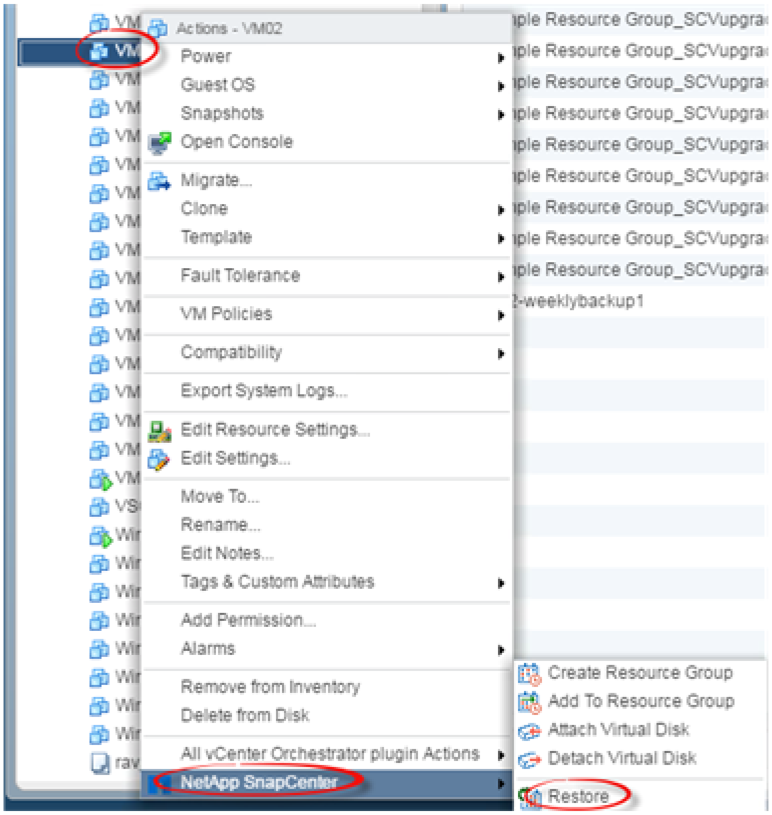
About this task

- If the VMDK is deleted or detached from the VM, then the restore operation attaches the VMDK to the VM.
- A restore operation might fail if the storage tier of the FabricPool where the VM is located is unavailable.
- Attach and restore operations connect VMDKs using the default SCSi controller. VMDKs that are attached to a VM with a NVME controller are backed up, but for attach and restore operations they are connected back using a SCSi controller.

Steps

1. In the VMware vSphere web client GUI, click 🏠 in the toolbar, and then select **VMs and Templates** from the drop-down list.

2. In the left Navigator pane, right-click a VM, then select **NetApp SnapCenter** in the drop-down list, and then select **Restore** in the secondary drop-down list.



3. In the **Restore** wizard, on the **Select Backup** page, select the backup copy that you want to restore from.

   You can search for a specific backup name or a partial backup name, or you can filter the backup list by clicking (filter icon) and selecting a date and time range, selecting whether you want backups that contain VMware Snapshots, whether you want mounted back ups, and primary or secondary location. Click **OK** to return to the wizard.

4. On the **Select Scope** page, select the restore destination by clicking **Particular virtual disk** in the **Restore scope** field.

To...	Specify the restore destination...
Restore to the original datastore	Use the default, parent, datastore that is displayed.
Restore to an alternate datastore	Click on the destination datastore and select a different datastore from the list.

   You can unselect any datastores that contain VMDKs that you do not want to restore.

5. On the **Select Location** page, select the Snapshot copy that you want to restore (primary or secondary).

6. Review the Summary page and then click **Finish**.

7. Optional: Monitor the operation progress by clicking **Recent Tasks** at the bottom of the screen.

   Refresh the screen to display updated information.

Related concepts

How restore operations are performed on page 37

Restoring guest files and folders

You can restore files or folders from a virtual machine disk (VMDK) on a Windows guest OS.

Overview of steps in guest restore operations

1. Attaching a virtual disk to a guest VM or proxy VM and starting a guest file restore session.
2. Waiting for the attach operation to complete before you can browse and restore.
   When the attach operation finishes, a guest file restore session is automatically created and an email notification is sent.
3. Browsing the VMDK in the Guest File Restore session and selecting one or more files or folders to restore.
4. Restoring the selected files or folders to a specified location.

Guest file restore limitations

- You cannot restore dynamic disk types inside a guest OS.
- If you restore an encrypted file or folder, the encryption attribute is not retained. You cannot restore files or folders to an encrypted folder.
- The Guest File Browse page displays the hidden files and folder, which you cannot filter.
- Restoring from a Linux guest OS is not supported
  You cannot restore files and folders from a VM that is running Linux guest OS. For the latest information on supported guest OS, see the NetApp Interoperability Matrix.
  NetApp Interoperability Matrix Tool
- Restore operations from a NTFS file system to a FAT file system is not supported
  When you try to restore from NTFS-format to FAT-format, the NTFS security descriptor is not copied because the FAT file-system does not support Windows security attributes.
- You cannot restore guest files from a cloned VMDK.
- You cannot restore from secondary backups if the backup was performed on a system running ONTAP 9.2 or later and if the VMware consistency option was on.

Prerequisites for restoring guest files and folders

Before you restore one or more files or folders from a VMDK on a Windows guest OS, you must be aware of all the requirements.

- VMware Tools must be installed and running.
  SnapCenter uses information from VMware Tools to establish a connection to the VMware Guest OS.
- The Windows Guest OS must be running Windows Server 2008 R2 or later.
  For the latest information about supported versions, see the NetApp Interoperability Matrix Tool (IMT).
  NetApp Interoperability Matrix Tool
- The Run As credentials for the target VM must specify the built-in domain administrator account "administrator".
  Before starting the restore operation, Run As credentials must be configured for the VM to which you want to attach the virtual disk. The Run As credentials are required for both the attach operation and the subsequent restore operation.

> **Note:** Workgroup or local administrator privileges are not valid for guest file restore operations.
>
> **Attention:** If you must use any other domain account that is not built-in, you must disable UAC on the guest VM.

- You must know the backup Snapshot copy and VMDK to restore from.
  SnapCenter Plug-in for VMware vSphere does not support searching of files or folders to restore. Therefore, before you begin you must know the location of the files or folders with respect to the Snapshot copy and the corresponding VMDK.
- Virtual disk to be attached must be in a SnapCenter backup.
  The virtual disk that contains the file or folder you want to restore must be in a VM backup that was performed using SnapCenter Plug-in for VMware vSphere.
- To use a proxy VM, the proxy VM must be configured.
  If you want to attach a virtual disk to a proxy VM, the proxy VM must be configured before the attach and restore operation begins.
- You must restore files with non-English-alphabet names in a directory, not as a single file.
  You can restore files with non-alphabetic names, such as Japanese Kanji, by restoring the directory in which the files are located.
- Restoring from a Linux guest OS is not supported
  You cannot restore files and folders from a VM that is running Linux guest OS. For the latest information on supported guest OS, see the NetApp Interoperability Matrix.
  NetApp Interoperability Matrix Tool

Restoring guest files and folders from VMDKs

You can restore one or more files or folders from a VMDK on a Windows guest OS.

About this task

By default, the attached virtual disk is available for 24 hours and then it is automatically detached. You can choose in the wizard to have the session automatically deleted when the restore operation completes, or you can manually delete the Guest File Restore session at any time, or you can extend the time in the **Guest Configuration** page.

Guest file or folder restore performance depends upon two factors: the size of the files or folders being restored; and the number of files or folders being restored. Restoring a large number of small-sized files might take a longer time than anticipated compared to restoring a small number of large-sized files, if the data set to be restored is of same size.

> **Attention:** Only one attach or restore operation can run at the same time on a VM. You cannot run parallel attach or restore operations on the same VM.
>
> **Attention:** The guest restore feature allows you to view and restore system and hidden files and to view encrypted files. Do not attempt to overwrite an existing system file or to restore encrypted files to an encrypted folder. During the restore operation, the hidden, system, and encrypted attributes of guest files are not retained in the restored file.

Steps

1. In the VMware vSphere web client in vCenter, click 🏠 > **VMs and Templates** then right-click a VM, select **NetApp SnapCenter** from the drop-down list, and then select **Guest File Restore** from the secondary drop-down list.

   Select the VM where you want to attach the virtual disk. If you do not want to attach directly to that VM, you can select a proxy VM in the wizard.

Before you start the wizard, make sure the target VM for the guest file restore operation has valid Run As credentials.

The Guest File Restore wizard begins.

2. In the **Restore Scope** page in the wizard, specify the backup that contains the virtual disk you want to attach by doing the following:

   a. In the **Backup Name** table, select the backup that contains the virtual disk that you want attach.

   b. In the **VMDK** table, select the virtual disk that contains the files or folders you want to restore.

   c. In the **Locations** table, select the location, primary or secondary, of the virtual disk that you want to attach.

3. In the **Guest Details** page in the wizard, do the following:

   a. Choose where to attach the virtual disk by doing the following:

Select this option…	If…
Use Guest VM	You want to attach the virtual disk to the VM that you right-clicked before you started the wizard, and then select the Run As credential for the VM. **Note:** Run As credentials must already be created for the VM.
Use Guest File Restore proxy VM	You want to attach the virtual disk to a proxy VM and then select the proxy VM. **Note:** The proxy VM must be configured before the attach and restore operation begins.

   b. Select the **Send email notification** option.

   This option is required if you want to be notified when the attach operation completes and the virtual disk is available. The notification email includes the virtual disk name, the VM name, and the newly assigned drive letter for the VMDK.

   > **Best Practice:** Enable this option because a guest file restore is an asychronous operation and there might be a time latency to establish a guest session for you.

   This option uses the email settings that are configured when you set up the VMware vSphere web client in vCenter.

4. Review the summary, and then click **Finish**.

   Before you click **Finish**, you can go back to any page in the wizard and change the information.

5. Wait until the attach operation completes.

   You can view the progress of the attach operation in the Guest File Restore page, or in the Dashboard job monitor, or you can wait for the email notification.

6. To find the files that you want to restore from the attached virtual disk, click 🏠 > **SnapCenter Plug-in for VMware vSphere**, then in the left Navigator pane click **Guest File Restore** and select the **Guest Configuration** tab.

   In the Guest Session Monitor table, you can display additional information about a session by clicking **...** in the right column.

7. Select the guest file restore session for the virtual disk that was listed in the notification email.

   All partitions are assigned a drive letter, including system reserved partitions. If a VMDK has multiple partitions, you can select a specific drive by selecting the drive in the drop-down list in the drive field at the top of the Guest File Browse page.

8. Click the **Browse Files** icon to view a list of files and folders on the virtual disk.

   When you double click a folder to browse and select individual files, there might be a time latency while fetching the list of files because the fetch operation is performed at run time.

   For easier browsing, you can use filters in your search string. The filters are case-sensitive, Perl expressions without spaces. The default search string is `.*`. The following table shows some example Perl search expressions.

This expression....	Searches for...
`.`	Any character except a newline character.
`.*`	Any string. This is the default.
`a`	The character `a`.
`ab`	The string `ab`.
`a|b`	The character `a` or `b`.
`a*`	Zero or more instances of the character `a`.
`a+`	One or more instances of the character `a`.
`a?`	Zero or one instance of the character `a`.
`a{x}`	Exactly *x* number of instances of the character `a`.
`a{x,}`	At least *x* number of instances of the character `a`.
`a{x,y}`	At least *x* number of instances of the character `a` and at most *y* number.
`\`	Escapes a special character.

   Note: The Guest File Browse page displays all hidden files and folders. in addition to all other files and folders.

9. Select one or more files or folders that you want to restore, and then click **Select Restore Location**.

   The files and folders to be restored are listed in the Selected File(s) table.

10. In the **Select Restore Location** page, specify the following:

Option	Description
Restore to path	Enter the UNC share path to the guest where the selected files will be restored. For example: `\\10.60.136.65\c$`
If original file(s) exist	Select the action to be taken if the file or folder to be restored already exists on the restore destination: Always overwrite or Always skip. **Note:** If the folder already exsits, then the contents of the folder are merged with the existing folder.
Disconnect Guest Session after successful restore	Select this option if you want the guest file restore session to be deleted when the restore operation completes.

11. Click **Restore**

    You can view the progress of the restore operation in the Guest File Restore page, or in the Dashboard job monitor, or you can wait for the email notification. The time it takes for the email notification to be sent depends upon the length of time of the restore operation.

    The notification email contains an attachment with the output from the restore operation. If the restore operation fails, open the attachment for additional information.

Result

If the guest file restore operation fails, you must clear out the SnapMirror restore relationship (RST) that remains by using the `snapmirror restore -clean-up-failure` command. If you do not clear the relationship, subsequent backup and restore operations will also fail.

Related concepts

How restore operations are performed on page 37

Related tasks

Configuring Run As credentials for VM guest file restores on page 48
Setting up proxy VMs for restore operations on page 48

Setting up proxy VMs for restore operations

If you want to use a proxy VM for attaching a virtual disk for guest file restore operations, you must set up the proxy VM before you begin the restore operation. Although you can set up a proxy VM at any time, it might be more convenient to set it up immediately after the plug-in installation completes.

Steps

1. In the VMware vSphere web client in vCenter, click 🏠 in the toolbar, and then select **SnapCenter Plug-in for VMware** from the drop-down list.
2. In the left Navigator pane, click **Guest File Restore**.
3. In the **Run As Credentials** section, either select a configured Run As credentials from the list or click ➕ (Add) to add new Run As credentials.

   Windows uses the selected Run As credentials to log into the selected proxy VM.

   Note: The Run As credentials must be the default domain administrator that is provided by Windows. Any other user with administrator privileges will not work.
4. In the **Proxy Credentials** section, click ➕ (Add) to add a VM to use as a proxy.
5. In the **Proxy VM** dialog box, complete the information, and then click **Save**.

Configuring Run As credentials for VM guest file restores

When you attach a virtual disk for guest file or folder restore operations, the target VM for the attach must have Run As credentials configured before you restore.

Steps

1. In the VMware vSphere web client in vCenter, click 🏠 in the toolbar, and then select **SnapCenter Plug-in for VMware** from the drop-down list.

2. In the left Navigator pane, click **Guest File Restore**.
3. In the **Run As Credentials** section, either select a configured Run As credentials from the list or click ✚ (Add) to add new Run As credentials.

   Windows uses the selected Run As credentials to log into the selected VM.

   Note: The Run As credentials must be the default domain administrator that is provided by Windows. Any other user with administrator privileges will not work.
4. Click **Save**.

Extending the time of a guest file restore session

By default, an attached Guest File Restore VMDK is available for 24 hours and then it is automatically detached. You can extend the time in the **Guest Configuration** page.

About this task

You might want to extend a guest file restore session if you want to restore additional files or folders from the attached VMDK at a later time. However, because guest file restore sessions use a lot of resources, extending session time should be performed only occasionally.

Steps

1. In the VMware vSphere web client in vCenter, click 🏠 in the toolbar, and then select **SnapCenter Plug-in for VMware** from the drop-down list.
2. In the left Navigator pane, click **Guest File Restore**.
3. Select a guest file restore session and then click ⤢ (Extend Selected Guest Session) in the Guest Session Monitor title bar.

   The session is extended for another 24 hours.

Manually deleting a guest file restore session

By default, an attached Guest File Restore VMDK is available for 24 hours and then it is automatically detached. You can choose in the wizard to have the session automatically deleted when the guest file restore operation completes, or you can manually delete the Guest File Restore session at any time.

About this task

You might want to manually delete a guest file restore session after you have extended the session time and you have completed all your restore operations and you do not want to wait until the session is deleted automatically.

Steps

1. In the left Navigator pane of the VMware vSphere web client in vCenter for the Plug-in for VMware vSphere,, click **Guest File Restore**.
2. Select a guest file restore session and then click 🗑 in the Guest Session Monitor title bar.

Attaching VMDKs to a VM

You can attach one or more VMDKs from a backup to the parent VM or to an alternate VM. This makes it easier to restore one or more individual files from a drive instead of restoring the entire drive. You can detach the VMDK after you have restored or accessed the files you need.

About this task

You have the following attach options:

- You can attach virtual disks from a primary or a secondary backup.
- You can attach virtual disks to the parent VM (the same VM that the virtual disk was originally associated with) or to an alternate VM.

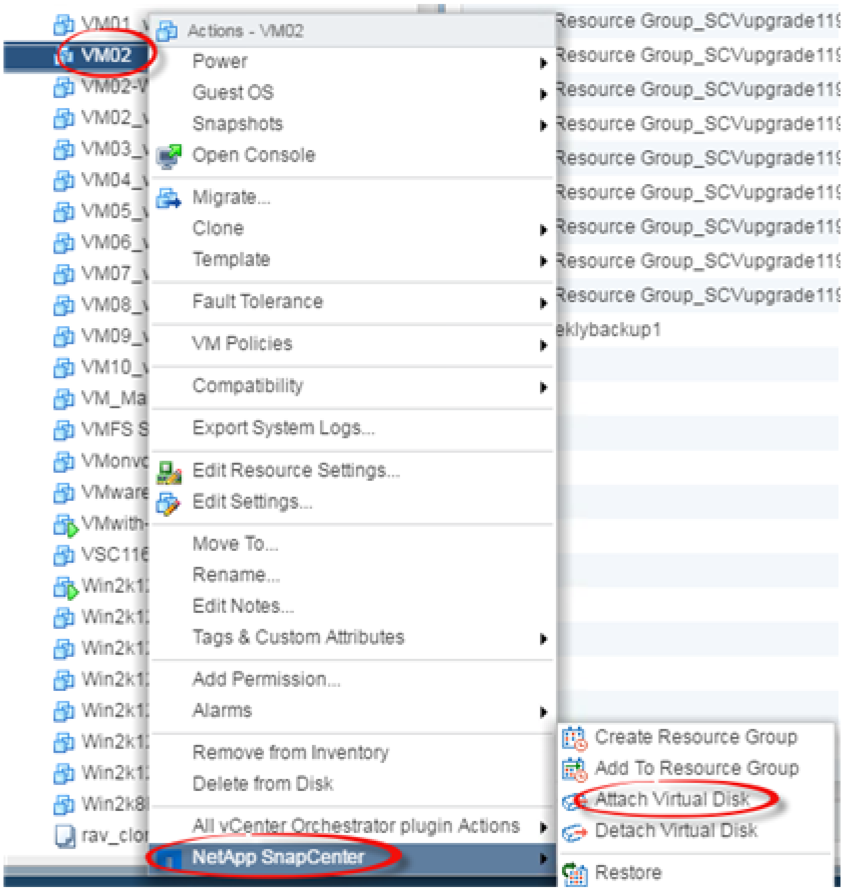
The following limitations apply to attaching virtual disks:

- Attach and detach operations are not supported for Virtual Machine Templates.
- When more than 15 VMDKs are attached to an iSCSI controller, SnapCenter Plug-in for VMware vSphere cannot locate VMDK unit numbers higher than 15 due to VMware restrictions.
  In this case, add the SCSi controllers manually and try the attach operation again.
- You cannot manually attach a virtual disk that was attached or mounted as part of a guest file restore operation.
- Attach and restore operations connect VMDKs using the default SCSi controller. VMDKs that are attached to a VM with a NVME controller are backed up, but for attach and restore operations they are connected back using a SCSi controller.

Steps

1. In the VMware vSphere web client GUI, click 🏠 in the toolbar, and then select **VMs and Templates** from the drop-down list.
2. Optional: In the left Navigator pane, select a VM.
3. Optional: Click the **Related Objects** tab (or **More Objects** in vCenter 6.5), then select the **Backups** tab to view the list of backups for the selected VM.

   Scroll right to see all the columns on the screen.
4. In the left navigation pane, right-click the VM, then select **NetApp SnapCenter** in the drop-down list, and then select **Attach virtual disk** in the secondary drop-down list.



5. On the **Attach Virtual Disk** pane, in the **Backup** section, select a backup.

   You can filter the backup list by clicking (filter icon) and selecting a date and time range, selecting whether you want backups that contain VMware snapshots, whether you want mounted back ups, and the location. Click **OK**.

6. On the **Attach Virtual Disk** pane, in the **Select Disks** section, select one or more disks you want to attach and the location you want to attach from (primary or secondary).

   You can change the filter to display primary and secondary locations.

7. By default, the selected virtual disks are attached to the parent VM. To attach the selected virtual disks to an alternate VM, click **Click here to attach to alternate VM** and specify the alternate VM.

8. Click **Attach**.

9. Optional: Monitor the operation progress in the **Recent Tasks** section.

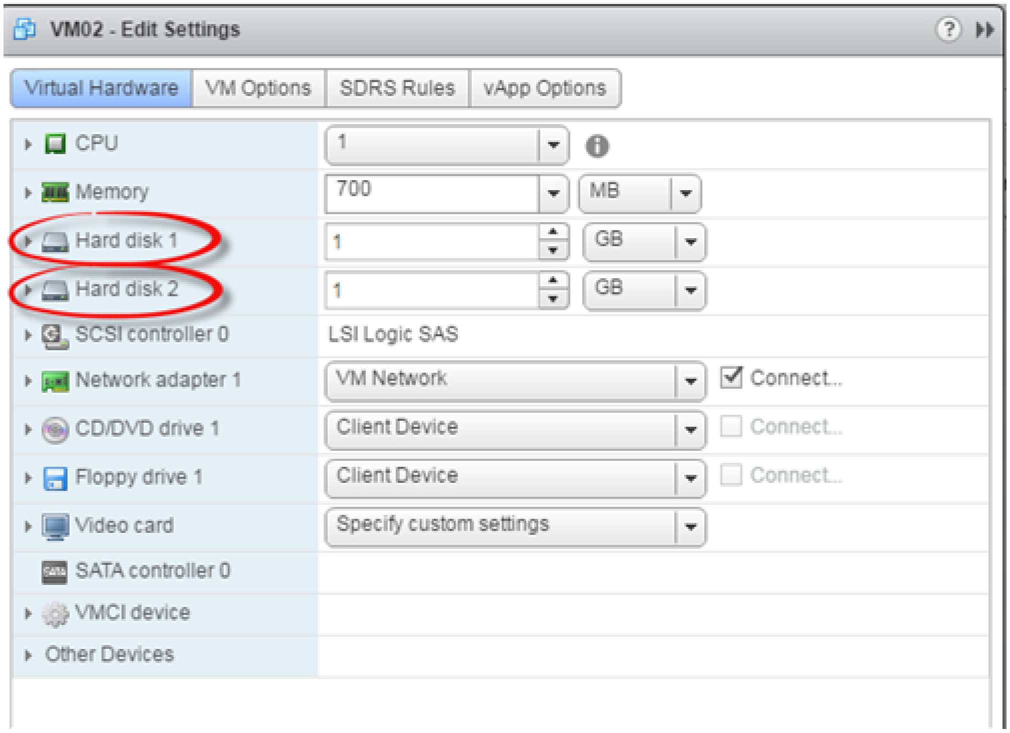
   Refresh the screen to display updated information.

10. Verify that the virtual disk is attached by performing the following:

    a. Click in the toolbar, and then select **VMs and Templates** from the drop-down list.

    b. In the left Navigator pane, right-click a VM, then select **Edit settings** in the drop-down list.

    c. In the **Edit Settings** box, click **Manage other disks** and then expand the list for each hard disk to see the list of disk files.



CPU	1		
Memory	700	MB	
Hard disk 1	1	GB	
Hard disk 2	1	GB	
SCSI controller 0	LSI Logic SAS		
Network adapter 1	VM Network		☑ Connect...
CD/DVD drive 1	Client Device		☐ Connect...
Floppy drive 1	Client Device		☐ Connect...
Video card	Specify custom settings		
SATA controller 0			
VMCI device			
Other Devices			

The Edit Settings page lists the disks on the VM. You can expand the details for each hard disk to see the list of attached virtual disks.

Result

You can access the attached disks from the host operating system and then retrieve the needed information from the disks.

Detaching a virtual disk

After you have attached a virtual disk to restore individual files, you can detach the virtual disk from the parent VM.

Steps

1. In the VMware vSphere web client GUI, click 🏠 in the toolbar, and then select **VMs and Templates** from the drop-down list.
2. Optional: In the left Navigator pane, select a VM.
3. Optional: Click the **Related Objects** tab (or **More Objects** in vCenter 6.5), then select the **Backups** tab to view the list of backups for the selected VM.

   Scroll right to see all the columns on the screen.
4. In the left navigation pane, right-click a VM, then select **NetApp SnapCenter** in the drop-down list, and then select **Detach virtual disk** in the secondary drop-down list.
5. On the **Detach Virtual Disk** screen, select one or more disks you want to detach, then click the **Detach the selected disk(s)** button, and then click **Confirm**.

   Attention: Make sure that you select the correct virtual disk. Otherwise, you might cause an impact on production work.

6. Optional: Monitor the operation progress in the **Recent Tasks** section.

   Refresh the screen to display updated information.

7. Verify that the virtual disk is detached by performing the following:

   a. Click 🏠, and then select **VMs and Templates** from the drop-down list.

   b. In the left Navigator pane, right-click a VM, then select **Edit settings** in the drop-down list.

   c. In the **Edit Settings** box, click **Manage other disks** and then expand the list for each hard disk to see the list of disk files.

   The Edit Settings page lists the disks on the VM. You can expand the details for each hard disk to see the list of attached virtual disks.

Mounting and unmounting datastores

You can mount a datastore from a backup if you want to access files in the backup. You can either mount the backup to the same ESXi host where the backup was created or to an alternate ESXi host that has the same type of VM and host configurations. You can mount a datastore multiple times on a host.

Mounting a datastore backup

You can manually mount a datastore backup if you want to access the files in the backup.

Before you begin

If you want to mount to an alternate ESXi host, you must ensure that the alternate ESXi host can connect to the storage.

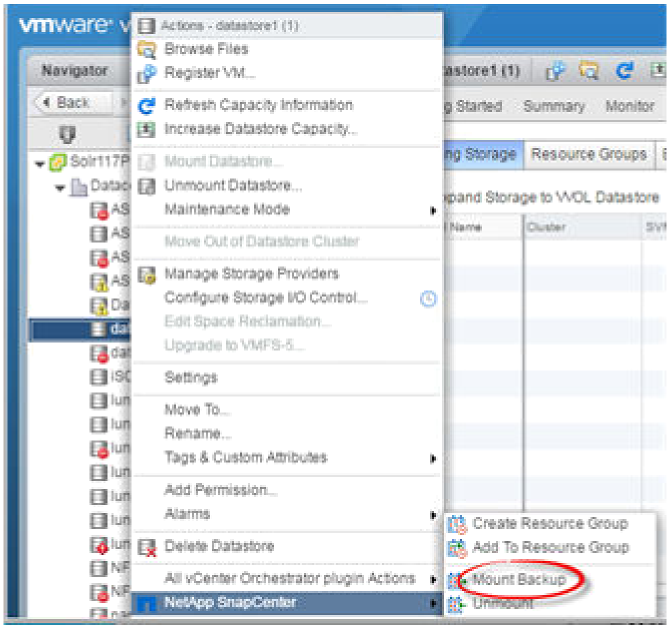
- Same UID and GID as that of the original host
- Same SnapCenter Plug-in for VMware vSphere version as that of original host

About this task

Note: A mount operation might fail if the storage tier of the FabricPool where the datastore is located is unavailable.

Steps

1. In the VMware vSphere web client GUI, click in the toolbar, and then select **Storage** from the drop-down list.
2. Right-click a datastore and select **NetApp SnapCenter** in the drop-down list, and then select **Mount Backup** in the secondary drop-down list.



3. On the **Mount Datastore** page, select a backup and a backup location, and then click **Finish**.

4. Optional: To verify that the datastore is mounted, perform the following:
    a. Click 🏠 in the toolbar, and then select **Storage** from the drop-down list.
    b. The left Navigator pane displays the datastore you mounted at the top of the list.

Unmounting a datastore backup

You can unmount a datastore backup when you no longer need to access the files in the datastore.

Steps

1. In the VMware vSphere web client GUI, click 🏠 in the toolbar, and then select **Storage** from the drop-down list.
2. In the left Navigator pane, right-click a datastore, then select **NetApp SnapCenter** in the drop-down list, and then select **Unmount** in the secondary drop-down list.

    Attention: Make sure that you select the correct datastore to unmount. Otherwise, you might cause an impact on production work.

3. In the **Unmount Cloned Datastore** dialog box, click the **Unmount the cloned datastore** option, and then click **Confirm**.

Managing SVMs in the SnapCenter Plug-in for VMware vSphere inventory

Before you can backup or restore VMs, you must add the SVMs on which the VMs are located. You can use either the SnapCenter GUI or the SnapCenter Plug-in for VMware vSphere GUI to add the SVMs.

Modifying SVMs using the SnapCenter Plug-in for VMware vSphere GUI

You can use either the SnapCenter GUI or the SnapCenter Plug-in for VMware vSphere GUI to modify SVMs in vCenter.

Steps

1. In the left Navigator pane of the VMware vSphere web client in vCenter for the Plug-in for VMware vSphere, click **Storage Systems**.
2. On the **Storage Systems** page, select the SVM to be modified and then click ✏ **Edit Storage System**.
3. On the **Edit Storage System** dialog box, enter the new values, and then click **Add** to apply the changes.

Removing SVMs using the SnapCenter Plug-in for VMware vSphere GUI

You can use either the SnapCenter GUI or the SnapCenter Plug-in for VMware vSphere GUI to remove SVMs from the inventory in vCenter and SnapCenter.

Before you begin

The SnapCenter Plug-in for VMware vSphere host to be removed must not have any mounted datastores. You must unmount all datastores in the SVM before you can remove the SVM.

About this task

Note: If a resource group has backups that reside on an SVM that you remove, then subsequent backups for that resource group fail.

Steps

1. In the left Navigator pane of the VMware vSphere web client in vCenter for the Plug-in for VMware vSphere, click **Storage Systems**.
2. On the **Storage Systems** page, select the SVM to be removed and then click ❌ **Remove**.
3. In the **Remove Storage System** confirmation box, click **Yes** to confirm.

Managing resource groups for VMs and datastores

You can create, modify, and delete backup resource groups, and perform backup operations on resource groups.

You can perform the following tasks on resource groups for VMs and datastores:

- Suspend and resume scheduled operations on the resource group
- Create a resource group
- Add VMs or datastores to a resource group
- Delete VMs or datastores from a resource group
- Modify a resource group
- Create a backup using the resource group
- Delete a resource group

Note: Resource groups were called *backup jobs* in Virtual Storage Console (VSC).

Related tasks

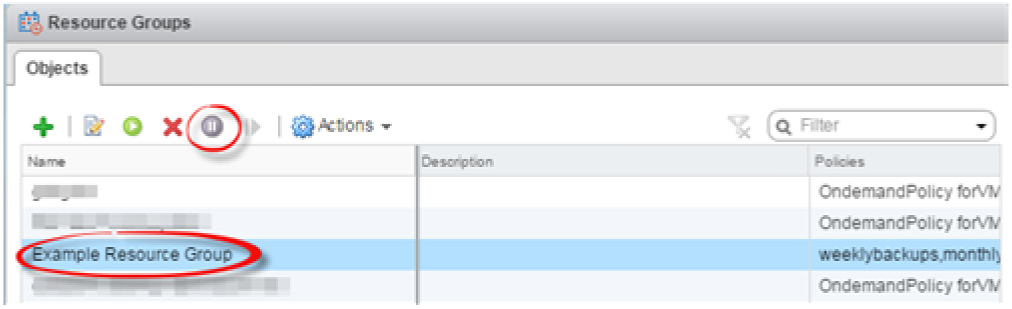
Creating resource groups for VMs and datastores on page 31
Adding a single VM or datastore to a resource group on page 34
Backing up VM and datastore resource groups on demand on page 35

Suspending and resuming operations on resource groups

You can temporarily disable scheduled operations from starting on a resource group. Later when you want, you can enable those operations.

Steps

1. In the left Navigator pane of the VMware vSphere web client in vCenter for the Plug-in for VMware vSphere, click **Resource Groups**.
2. On the **Resource Groups** page, on the **Objects** tab, select a resource group in the table and click ⏸ (Suspend).



Name	Description	Policies
[redacted]		OndemandPolicy forVM
[redacted]		OndemandPolicy forVM
Example Resource Group		weeklybackups,monthly
[redacted]		OndemandPolicy forVM

3. In the **Suspend resource group** confirmation box, click **Yes** to confirm.

After you finish

On the Resource Groups page, the job status for the suspended resource is `Under_Maintenance`. You might need to scroll to the right of the table to see the Job Status column.

To resume backup operations, select the resource group, and then click ▶ (Resume). After backup operations are resumed, the Job Status changes to `Production`.

Modifying resource groups

You can remove or add resources in resource groups, detach or attach policies, modify schedules, or modify any other resource group option.

About this task

If you want to modify the name of a resource group, do not use the following special characters in VM, datastore, policy, backup, or resource group names:

% & * $ # @ ! \ / : * ? " < > - | ; ' , . An underscore character (_) is allowed.

Steps

1. In the left Navigator pane of the VMware vSphere web client in vCenter for the Plug-in for VMware vSphere, click **Resource Groups**.
2. On the **Resource Groups** page, on the **Objects** tab, select a resource group in the table and then click ✏ (Edit).
3. On the left list in the **Edit Resource Group** wizard, click **Resources**.
4. Do one of the following:

If you want to....	Then do the following...
Remove a resource from the group	**a.** Select a VM or datastore on Selected Entities list. **b.** Click the left arrow (<) to remove it from the resource group.
Add a resource to the group	**a.** Select a VM or datastore on Available Entities list. **b.** Click the right arrow (>) to add it to the resource group.

5. Click **Next** until you see the **Summary** page, and then click **Finish**.

Related tasks

Adding a single VM or datastore to a resource group on page 34
Adding multiple VMs and datastores to a resource group on page 35

Deleting resource groups

You can delete a resource group if you no longer need to protect the resources in the resource group. You must ensure that all resource groups are deleted before you remove plug-ins from vCenter or SnapCenter.

About this task

All resource group delete operations are performed as force deletes. The delete operation detaches all policies from the resource group, removes the resource group from SnapCenter Plug-in for VMware vSphere, and deletes all backups and Snapshot copies of the resource group.

Note: In a SnapVault relationship, the last Snapshot copy cannot be deleted; therefore, the resource group cannot be deleted. Before deleting a resource group that is part of a SnapVault relationship, you must use either OnCommand System Manager or use the ONTAP CLI to remove the SnapVault relationship, and then you must delete the last Snapshot copy.

Steps

1. In the left Navigator pane of the VMware vSphere web client in vCenter for the Plug-in for VMware vSphere, click **Resource Groups**.
2. On the **Resource Groups** page, on the **Objects** tab, select a resource group in the table and click ✖ (Delete).
3. In the **Delete resource group** confirmation box, click **Yes** to confirm.

Managing policies for VMs and datastores

You can create, modify, view, detach, and delete backup policies. Policies are required to perform data protection operations.

Related tasks

Creating backup policies for VMs and datastores on page 26

Detaching policies

You can detach policies from a resource group when you no longer want those policies to govern data protection for the resources. You must detach a policy before you can remove it or before you modify the schedule frequency.

About this task

Attention: The guidelines for detaching policies from SnapCenter Plug-in for VMware vSphere resource groups in the VMware vSphere web client differ from the guidelines for SnapCenter resource groups. For a VMware vSphere web client resource group, you can detach all policies, which leaves the resource group with no policy. However, to perform any data protection operations on that resource group, you need to attach at least one policy.

Steps

1. In the left Navigator pane of the VMware vSphere web client in vCenter for the Plug-in for VMware vSphere, click **Resource Groups**.
2. In the **Resource Groups** page, select a resource group, and then click ✎ (Edit).
3. On the **Policies** page of the **Edit Resource Group** wizard, clear the check mark next to the policies you want to detach.

   You can also add a policy to the resource group by checking the policy.
4. Make any additional modifications to the resource group in the rest of the wizard, and then click **Finish**.

Modifying policies

You can modify the frequency, replication options, Snapshot copy retention settings, or scripts information while a policy is attached to a resource group.

About this task

Modifying SnapCenter Plug-in for VMware vSphere backup policies in the VMware vSphere web client differs from modifying backup policies in the SnapCenter GUI. You do not need to detach policies from resource groups when you modify policies in vCenter.

Before you modify the replication or retention settings, you should consider the possible consequences.

- Increasing replication or retention settings

  Backups continue to accumulate until they reach the new setting.

- Decreasing replication or retention settings
  Backups in excess of the new setting are deleted when the next backup is performed.

Note: To modify a policy schedule, you must modify the schedule in a resource group.

Steps

1. In the left Navigator pane of the VMware vSphere web client in vCenter for the Plug-in for VMware vSphere, click **Policies**.
2. On the **Policies** page, select a policy, and then click ✏ **Edit Policy** in the toolbar.
3. Modify the policy fields.
4. When you are finished, click **Update**.

Result

The changes take effect when the next scheduled backup is performed.

Related tasks

Modifying resource groups on page 58

Deleting policies

If you no longer require a policy in the VMware vSphere web client, you might want to delete it.

Before you begin

You must have detached the policy from all resource groups in the VMware vSphere web client before you can delete it.

Steps

1. In the left Navigator pane of the VMware vSphere web client in vCenter for the Plug-in for VMware vSphere, click **Policies**.
2. On the **Policies** page, select a policy, and then click ✖ **Remove** in the toolbar.
3. In the confirmation dialog box click **Yes**.

Managing backups of VMs and datastores

You can rename and delete backups performed by SnapCenter Plug-in for VMware vSphere in the VMware vSphere web client. You can also delete multiple backups simultaneously.

Related concepts

Backing up VMs, VMDKs, and datastores on page 24

Related tasks

Backing up VM and datastore resource groups on demand on page 35

Renaming backups

You can rename backups if you want to provide a better name to improve searchability.

Steps

1. In the VMware vSphere web client GUI, click 🏠 in the toolbar, and then select **VMs and Templates** from the drop-down list.
2. In the left Navigator pane, select a VM for which you want to rename a backup, then select the **Related Objects** tab (or **More Objects** in vCenter 6.5), and then select the **Backups** tab.
3. Select the backup that you want to rename and click ✏ **Rename**.
4. On the **Rename Backup** dialog box, enter the new name, and click **OK**.

   Do not use the following special characters in VM, datastore, policy, backup, or resource group names:

   % & * $ # @ ! \ / : * ? " < > - | ; ' , . An underscore character (_) is allowed.

Deleting backups

You can delete backups if you no longer require the backup for other data protection operations. You can delete one backup or delete multiple backups simultaneously.

Before you begin

You cannot delete backups that are mounted. You must unmount a backup before you can delete it.

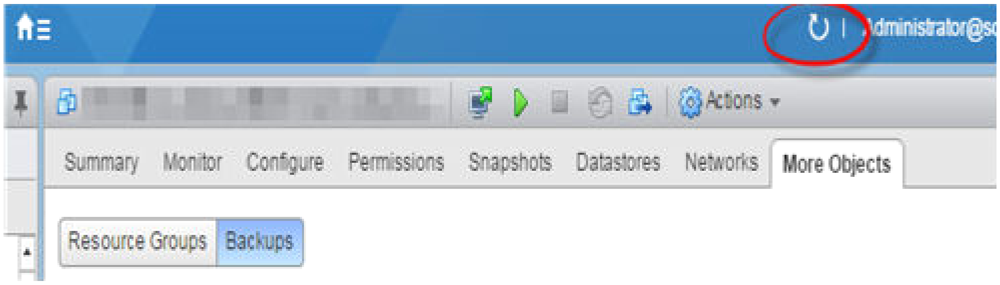
Steps

1. In the VMware vSphere web client GUI, click 🏠 in the toolbar, and then select **VMs and Templates** from the drop-down list.
2. In the left Navigator pane, select a VM, then select the **Related Objects** tab (or **More Objects** in vCenter 6.5), and then select the **Backups** tab.
3. Do one of the following:

To delete this many backups...	Do the following...
One	Select the backup and click ✖ **Delete**.
2 to 40	Select the backups, then click **Actions**, and then click ✖ **Delete** in the drop-down list. **Note:** You can select a maximum of 40 backups to delete.

4. Click **Yes** to confirm the delete operation.

5. Refresh the backup list by clicking the refresh button (a circled arrow) on the left vSphere menu bar.



Monitoring VMware vSphere web client status, jobs, and logs

Viewing jobs and log information for the SnapCenter VMware vSphere web client enables you to monitor your data protection status and use system log files for troubleshooting.

Dashboard for the VMware vSphere web client

The Dashboard in vCenter for the SnapCenter VMware vSphere web client displays the status of the installed plug-in, job status similar to that in the SnapCenter dashboard, and tabs for the Job Monitor, Reports, and Getting Started.

The Dashboard contains the following four tabs that display information for the selected vCenter Server:

- Status tab
    - Displays whether the SnapCenter Server and Plug-in for VMware vSphere are installed and the version each is running.
      A green checkmark indicates that the component is installed and registered successfully.
    - Displays an overview of the status of completed backup (primary and secondary), mount, and restore jobs. Status values are Completed, Warning, Failed, and Running. For definitions of the status terms used in each tile, click ℹ in the tile.
    - Displays the number of protected and unprotected VMs that are compatible with SnapCenter. For definitions of the status terms used in each tile, click ℹ in the tile.
      The Status tab displays only VMs that are compatible with SnapCenter. It does not display other VMs in vCenter that are incompatible with SnapCenter. For example, it does not display VMs that are running ONTAP in 7-Mode. You can view all VMs in the vCenter VMs and Templates page.

  Click a color portion of any graphic to jump to a more detailed graphic for that information on the Reports tab.
- Job Monitor tab
  Displays jobs and job details. You can download job logs for individual jobs or for all jobs.
- Reports tab
  Displays detailed graphic information for the selected report and lists the job IDs. Click (filter icon) to configure what you want the report to include: time range, job status type, resource groups, and policies.
- Getting Started tab
  Displays a graphic of the workflow for setting up the Plug-in for VMware vSphere.

The **Download Job Logs** button downloads all the job logs in the VMware vSphere web client Job Monitor tab.

Related tasks

Monitoring VMware vSphere web client jobs on page 65
Downloading VMware vSphere web client job logs on page 65

Monitoring VMware vSphere web client jobs

After performing any data protection operation using the VMware vSphere web client, you can monitor the job status from the Job Monitor tab in the Dashboard and view job details.

Steps

1. In the left navigator pane of the VMware vSphere web client, click **Dashboard** and then click the **Job Monitor** tab.

   The Job Monitor tab lists each job and its status, start time, and end time. If the job names are long, you might need to scroll to the right to view the start and end times. The display is refreshed every 30 seconds.

   - Click ↻ (refresh icon) to refresh the display on-demand.
   - Click ⧩ (filter icon) to select the time range, type, and status of jobs you want displayed.

2. To view the details of a job, double-click the job.

   Click ↻ (refresh icon) in the Job Details window to refresh the display while the job is running.

Downloading VMware vSphere web client job logs

After performing any data protection operation using the VMware vSphere web client, you can monitor the job status from the Dashboard tab and download job logs.

Steps

1. In the left navigator pane of the VMware vSphere web client, click **Dashboard** and then click the **Job Monitor** tab.

   The Job Monitor tab lists each job and its status, start time, and end time. If the job names are long, you might need to scroll to the right to view the start and end times. The display is refreshed every 30 seconds.

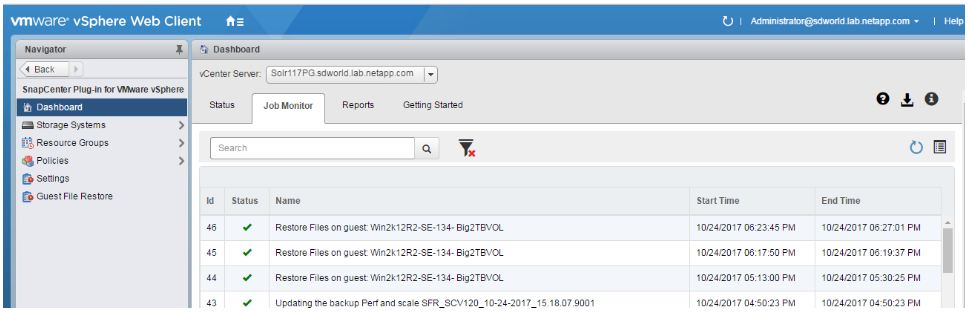
   - Refresh the display on-demand by clicking ↻ (refresh icon).
   - Click ⧩ (filter icon) to select the time range, type, and status of jobs you want displayed.

2. To download the job logs, do one of the following:

To download the logs for...	Perform the following...
A single job	**a.** Select a job **b.** Click ⬇ (download icon) in the search title bar. You might need to scroll to the right to see the icon. Or: **a.** Select a job **b.** Double-click the job to access the Job Details window, and then click **Download Job Logs**.
All jobs for the plug-in	Click ⬇ (download icon) in the **Job Monitor** title bar. You might need to scroll to the right to see the icon.

Result

Job logs are located on the local Windows host where SnapCenter Plug-in for VMware vSphere is installed. The default job log location is `C:\Program Files\NetApp\SnapCenter\SnapCenter Plugin for VMware vSphere\log`.



vCenter Server: Solr117PG.sdworld.lab.netapp.com

Id	Status	Name	Start Time	End Time
46	✓	Restore Files on guest: Win2k12R2-SE-134- Big2TBVOL	10/24/2017 06:23:45 PM	10/24/2017 06:27:01 PM
45	✓	Restore Files on guest: Win2k12R2-SE-134- Big2TBVOL	10/24/2017 06:17:50 PM	10/24/2017 06:19:37 PM
44	✓	Restore Files on guest: Win2k12R2-SE-134- Big2TBVOL	10/24/2017 05:13:00 PM	10/24/2017 05:30:25 PM
43	✓	Updating the backup Perf and scale SFR_SCV120_10-24-2017_15.18.07.9001	10/24/2017 04:50:23 PM	10/24/2017 04:50:23 PM

Using SnapCenter VMware vSphere web client reporting capabilities

The VMware vSphere web client provides a variety of reporting options that enable you to monitor and manage your system health and operation success.

Centralized reporting options for the VMware vSphere web client

The VMware vSphere web client makes it easy for you to monitor the health of your VMs and get more detailed information about data protection jobs.

Dashboard

The VMware vSphere web client Dashboard gives you a first glance into the status of your data protection jobs (backup, restore, and mount) and your VM protection status.

You can also request more detailed reports about data protection jobs by clicking any portion of a pie chart in the Dashboard. The report you generate from here pertains only to the type and status of the jobs you clicked.

For Backup Reports, you can click the (filter) icon to modify the time range, job status type, resource groups, and policies to be included in the report.

Reports tab

On the VMware vSphere web client Dashboard, the Reports tab offers a more detailed view into data protection jobs. You can run backup reports about all jobs of the selected type, jobs for a specific resource group, jobs for a specific policy, and jobs with a specific status (completed, failed, or warning). You can download reports in HTML or CSV format.

The Reports tab retains the report selection from the last time you viewed a report.

Attention: On the Reports tab, you can access backup reports only. You can access all report types by clicking a pie chart on the Dashboard.

Note: For backup jobs, the numbers in the Status tab for backup jobs might not match the numbers in the Reports tab. The Status tab lists all completed backup jobs. In contrast, the Reports tab includes only backup jobs that are still available.

For example, the Status tab might display a total of 142 successfully completed primary and secondary backup jobs during a selected time range. However, when you click the green successful portion of the graph, which jumps you to the Reports tab, the report might display only 20 successful backup jobs. This occurs because the retention settings in your backup policies caused some of the backup jobs to be deleted.

Information provided in VMware vSphere web client Dashboard reports

The VMware vSphere web client Dashboard gives you a first glance into the health of your VMs and the status of your data protection jobs, and makes it easy for you to generate reports.

Note: Icons in the dashboard or the Getting Started tab might change when you select the Plug-in for VMware vSphere home button. This does not change the functionality of the plug-in and the changed icons revert to the correct icons when the menu or dialog box closes.

Backup, restore, and mount job tiles

The backup, restore, and mount job tiles display information about the data protection jobs you have run during the specified time. You can customize the time frame for the report by changing the time frame located in each tile; the maximum value is 100 days. The default report provides information about data protection jobs run for the past seven days.

The job tiles are automatically updated every hour. To see the most recent information, click ↻ in the toolbar.

The default time range is seven days. You can modify the default time range in the tile on the Dashboard.

Note: For definitions of the status terms used in each tile, click ℹ in the tile.

VM Backup Status tile

The VM Backup Status tile displays information about the protection status of VMs that are compatible with SnapCenter.

The default time range is seven days. You can modify the default time range in the .override configuration file. See the section on overrides for customizing backup operations.

For definitions of the protection terms, click ℹ in the tile.

Types of reports

Report type	**Description**
Backup Report	The Backup Report displays overall data about successful backups created. For each backup, the report lists the backup name (Snapshot copy name), the corresponding resource group, and backup policy. On the Reports tab, you can double-click on a backup to generate a detailed report. Deleted backups are not included in the report.
Mount Report	The Mount Report displays overall data about mount trends for your SnapCenter environment. For each mount operation, the report lists the job ID, job status, job name, and job start and end times. The job name includes the Snapshot copy name. For example: `Mount Backup <`*`snapshot-copy-name`*`>`.

Report type	Description
Restore Report	The Restore Report displays overall information about restore jobs. For each restore operation, the report lists the job ID, job status, job name, and job start and end times. The job name includes the Snapshot copy name. For example: `Restore Backup <snapshot-copy-name>`.
Last Backup Status of VMs Report	These reports display the latest protection details for VMs managed by the Plug-in for VMware vSphere. The VM Backup Status Report for protected VMs displays details about the VM name, last successful Snapshot copy name, and start and end times for the latest backup run. The VM Backup Status Report for unprotected VMs displays the names of VMs that do not have any successful backups at the time the report was generated.

Related references

Overrides for customizing or retrying backup operations on page 79

Requesting reports from the VMware vSphere web client Dashboard

You can request reports for one or more VMware vSphere web client jobs from the Dashboard.

Steps

1. In the left navigator pane of the VMware vSphere web client, click **Dashboard**.
2. Click the **Status** tab, then click the portion of a pie chart for the job type you want.

   For example, you can click the portion of the pie chart for successful backup jobs. The Reports tab is displayed containing information for the job type and time range that you selected on the Status tab.
3. Optional: For Backup Reports, you can do the following:
   - Modify the report

     Click the ▼ (filter) icon to modify the time range, job status type, resource groups, and policies to be included in the report.
   - Generate a detailed report
     Double-click any job to generate a detailed report for that job.
4. Optional: On the **Reports** tab, click **Download**.

   You can download reports in HTML or CSV format.

Updating SnapCenter and vCenter settings

After you install SnapCenter, you might need to update the vCenter or SnapCenter configuration information for the SnapCenter Plug-in for VMware vSphere.

Updating hypervisor configuration settings

You can update your hypervisor configuration settings so that SnapCenter no longer displays a "configure hypervisor" message in the host status area.

Before you begin

- If you are using SnapCenter Plug-in for Microsoft SQL Server, your SQL Server environment must be using NFS or an iSCSI initiator.
- If you are using SnapCenter Plug-in for Oracle Database, your Oracle environment must be using NFS or an iSCSI initiator.

Steps

1. In the left navigation pane of the SnapCenter GUI, click **Settings**.
2. In the **Settings** page, click **Global Settings**.
3. In the **Hypervisor settings** area, select **VMs have iSCSI direct attached disks or NFS for all the hosts** and then click **Update**.

   The host status for the VM changes from “configure hypervisor” to “Running.”

Updating vCenter or SnapCenter information in the SnapCenter Plug-in for VMware vSphere

You might need to update the vCenter or SnapCenter host information that the SnapCenter Plug-in for VMware vSphere uses when communicating with vCenter. For example, an update might be necessary if the vCenter password for a host was changed.

Steps

1. In the left navigation pane of the SnapCenter GUI, click **Hosts**.
2. In the **Hosts** page, select the vSphere-type host.
3. Click the **Add/Update vCenter details** button.
4. In the dialog box, select the type of information you want to update:

   Add/Update vCenter Details
   Add/Update SnapCenter Details
5. In the dialog box, enter only the information that needs to be updated.

   Blank fields are not changed.
6. Click **OK**.

Troubleshooting

If you encounter unexpected behavior while performing data protection operations using the VMware vSphere web client, 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 download the log files using the VMware vSphere web client GUI in vCenter.

Related tasks

Monitoring VMware vSphere web client jobs on page 65

vCenter GUI not working correctly for SnapCenter Plug-in for VMware vSphere

Description

After a fresh install, or after an upgrade on a host 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 VMware vSphere web client GUI for the Plug-in for VMware vSphere does not match the documentation.

During normal use, a page display (for example, the Resource Groups page) may 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 in vCenter.

   Note: The steps for restarting the vSphere web client service are different depending upon the following:

   Platform: Windows or Linux
   vCenter version: 6.0 update 3 or later

Related tasks

Restarting the vSphere web client service in Windows on page 71
Restarting the vSphere web client service in Linux on page 72

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 vSphere 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:

      ```
      C:\Program Files\VMware\vCenter Server\vmon>.\vmon-cli --stop vsphere-client
      ```

      Wait for the message `Completed Stop service request`.

   b. Delete all stale packages on vCenter by performing the following:

      i. Navigate to the vCenter packages folder at `%PROGRAMDATA%/VMware/vCenterServer/cfg/vsphere-client/vc-packages/vsphere-client-serenity`

      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:

      ```
      C:\Program Files\VMware\vCenter Server\vmon>.\vmon-cli --start vsphere-client
      ```

      Wait for the message `Completed Start service request.`.

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

   a. Open Server Manager on the Windows system on which vCenter Server is running.

   b. Click **Configuration** > **Services**.

   c. Select **VMware vSphere Web Client** and click **Stop**.

   d. Delete all stale packages on vCenter by performing the following:

      i. Navigate to the vCenter packages folder at `%PROGRAMDATA%/VMware/vCenterServer/cfg/vsphere-client/vc-packages/vsphere-client-serenity`

      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**.

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 vSphere web client service.

Steps

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

   a. Use SSH to log in to the vCenter Server Appliance as root.

   b. Access the Appliance Shell or BASH Shell by using the following command:

      ```
      shell
      ```

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

      ```
      service-control --stop vsphere-client
      ```

   d. Delete all stale packages on vCenter by using the following command:

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

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

```
service-control --start vsphere-client
```

2. If you are running vCenter 6.0 update 3 or later, perform the following:
    a. Use SSH to log in to the vCenter Server Appliance as root.
    b. Access the Appliance Shell or BASH Shell by using the following command:
    ```
    shell
    ```
    c. Navigate to the directory by using the following command:
    ```
    cd /bin
    ```
    d. Stop the web client service by using the following command:
    ```
    service-control --stop vsphere-client
    ```
    e. Delete all stale packages on vCenter by using the following command:
    ```
    /etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity/
    ```
    f. Start the web client service by using the following command:
    ```
    service-control --start vsphere-client
    ```

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 SnapCenter Plug-in for VMware vSphere. SnapCenter Plug-in for VMware vSphere 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

You must add an SVM with a management LIF before you can perform backup or restore operations.

VMware vSphere does not remove snapshot delta disks during restore

Description

When you restore a backup of a VM on a Windows 2008 or Windows 2008 R2 system, SnapCenter Plug-in for VMware vSphere does not always remove all snapshot delta disks.

During a backup, SnapCenter Plug-in for VMware vSphere creates the quiesced VMware snapshot, which results in the creation of snapshot delta disks. However, if you restore the VM, revert to the VMware snapshot taken during the backup process, and then delete it, not all the delta disk files are deleted.

Corrective action

There is no workaround for this issue. You might want to contact VMware support for assistance.

SnapCenter compatibility check fails

Description

A SnapCenter compatibility check failed when you attempted to create a resource group. Reasons for incompatibility might be:

- VMDKs are on unsupported storage; for example, on an ONTAP system running in 7-Mode or on a non-ONTAP device.
- A datastore is on NetApp storage running Clustered Data ONTAP 8.2.1 or earlier.
  SnapCenter 3.0 supports ONTAP 8.2.2 and later. SnapCenter versions 3.0.1 and 4.0 support ONTAP 8.3.1 and later.
  The SnapCenter Plug-in for VMware vSphere does not perform compatibility checks for all ONTAP versions; only for ONTAP versions 8.2.1 and earlier. Therefore, always see the Interoprability Matrix Tool (IMT) for the latest information about SnapCenter support.
  NetApp Interoperability Matrix Tool
- A shared PCI device is attached to a VM.
- A preferred IP is not configured in SnapCenter.
- You have not added the SVM management IP to SnapCenter.
- The SVM is down.

Error message

`Some entities are not SnapCenter compatible`

Corrective actions

- Make sure the SVM is running.
- Make sure that the storage system on which the VMs are located have been added to the SnapCenter Plug-in for VMware vSphere inventory.
- Make sure the SVM is added to SnapCenter. Use the **Add storage system** option on the SnapCenter GUI or on the VMware vSphere web client GUI.

- If there are spanning VMs that have VMDKs on both NetApp and non-NetApp datastores, then move the VMDKs to NetApp datastores.

Backup fails with error: Storage system(s) may need to be added, also ensure that the associated host is in a connected state

Description

A backup failed because the preferred IP address that was configured for the SVM went down. When the preferred IP comes up again, the SnapCenter cache is not automatically refreshed. Therefore, SnapCenter could not find the Preferred IP when attempting to perform the backup.

Corrective action

Refresh the SnapCenter cache for the SVM:

1. In the left navigation pane of the SnapCenter GUI, click **Storage Systems**.
2. In the Storage Systems page, select the storage system used by the backup, and then click **Modify**.
3. Make sure that the **Preferred IP** check box is selected and that the IP is correct.
4. Reenter the storage system password, and then click **OK**.
   This action refreshes the SnapCenter cache and updates the storage system configuration.

Backup fails for version-flexible mirror for VM on NFS datastore

Description

A SnapMirror update failed for a Version-FlexibleMirror relationship for a VM on an NFS datastore.

Corrective action

To successfully transfer Snapshot copies to secondary storage for Version-FlexibleMirror relationships, make sure that the SnapMirror policy type is Asynchronous Mirror and that the "all_source_snapshots" option is checked.

Backups are not detached after guest file restore session is discontinued

Description

A guest file restore operation was performed from a VM-consistent backup. While the guest file restore session was active, another VM-consistent backup was performed for the same VM. When the guest file restore session is disconnected, either manually or automatically after 24 hours, the backups for the session are not detached.

Corrective action

You must manually detach the VMDKs that were attached from the active guest file restore session.

Unable to find Snapshot copy after successfully creating the backup

Description

While performing backup operations with SnapVault or SnapMirror update enabled, an error might be displayed stating that a Snapshot copy could not be found on the destination storage system.

The issue occurs when the plug-in performs a query for the destination Snapshot copy while the status of the SnapMirror or SnapVault operation is pending idle.

Corrective action

You must include the following parameters and specify the value in the `appsetting` section of the `SMCoreServiceHost.exe.Config` file located under `SmCore` in the SnapCenter Server.

- <add key="`SnapmirrorRetry`" value=*`retry_value`*/>
- <add key="`SnapmirrorTimeout`" value=*`timeout_value`*/>

The value assigned to `SnapmirrorRetry` defines the maximum number of checks that can done to identify whether the SnapMirror is transferred. The value (milliseconds) assigned to `SnapmirrorTimeout` defines the time lapse after each check.

Registering vCenter details task displays a warning

Description

You added a vSphere type of host and the Add Host operation completed successfully. However, the SnapCenter Plug-in for VMware vSphere was not able to communicate with the vCenter using the vCenter information you entered. The task "Registering vCenter details with SnapCenter Plug-in for VMware vSphere" in the operation details displays error information and is marked with a warning.

Task marked with a warning

`Registering vCenter details with SnapCenter Plug-in for VMware vSphere`.

Corrective action

Perform the following steps to update the vCenter information in the SnapCenter Plug-in for VMware vSphere:

1. In the left navigation pane, click **Hosts**.
2. In the Hosts page, select the vSphere-type host.
3. Click the **Add/Update vCenter details** button.
4. In the dialog box, select the type of information you want to update:

   Add/Update vCenter Details
   Add/Update SnapCenter Details

5. In the dialog box, enter only the information that needs to be updated. Blank fields are not changed.
6. Click **OK**.

Too many Snapshot copies after attach or mount operations

Description

If you perform an attach or mount operation on a SnapVault destination volume that is protected by SnapVault schedules and is running ONTAP 8.2.4, you may see an extra Snapshot copy listed in the attach or mount dialog screen. This occurs because the attach or mount operation clones the SnapVault destination volume and ONTAP updates the volume by creating a new Snapshot copy.

Corrective action

Turn off the ONTAP schedule for the SnapVault volume to prevent new Shapshot copies from being created when you clone the volume. Previously existing Snapshot copies are not deleted.

Guest file restore session is blank

Description

You created a guest file restore session and while that session was active, the guest operating system was rebooted. When this occurs, VMDKs in the guest OS might remain offline. Therefore, when you try to browse the guest file restore session, the list is blank.

Corrective action

Manually put the VMDKs back online in the guest OS. When the VMDKs are online, the guest file restore session will display the correct contents.

Guest file restore attach disk operation fails

Description

You started a guest file restore operation but the attach disk operation failed even though VMware Tools was running and the Guest OS credentials were correct.

Error

```
Error while validating guest credentials, failed to access guest
system using specified credentials: Please verify VMWare tools is running
properly on system and account used is Administrator account,
Error is SystemError vix error codes = (3016, 0).
```

Corrective action

Restart the VMware Tools Windows service on the Guest OS, and then retry the guest file restore operation.

Guest file restore email shows ?????? for file name in email

Description

You used the guest file restore feature to restore files or folders with non-English characters in the names and the email notification displays "??????" for the restored file names.

Corrective action

The email attachment correctly lists the names of the restored files and folders.

Appendices

These appendices provide additional reference information for SnapCenter users.

Overrides for customizing or retrying backup operations

To improve operational efficiency, you can modify the `scbr.override` configuration file to change the default values. These values control settings such as the number of VMware snapshots that are created or deleted during a backup or the amount of time before a backup script stops running.

The `scbr.override` configuration file is used in SnapCenter Plug-in for VMware vSphere environments that support SnapCenter.

If this file does not exist, you must create it in the `C:\Program Files\NetApp\SnapCenter\SnapCenter Plugin for VMware\etc\scbr` directory.

You must restart the SnapCenter Plug-in for VMware vSphere Windows service for the changes to take effect.

Values that you can change in the `scbr.override` configuration file

You can modify the default values for the following properties. Each of the default values is shown with the property.

Note: The values that you can override are also listed in the file `C:\Program Files\NetApp\Virtual Storage Console\etc\scbr\scbr.override-template`.

`dashboard.protected.vm.count.interval=7`

Specifies the number of days for which the dashboard displays VM protection status.

The default value is "7."

`guestFileRestore.guest.operation.interval=5`

Specifies the time interval, in seconds, that SnapCenter Plug-in for VMware vSphere monitors for completion of guest operations on the guest (Online Disk and Restore Files). The total wait time is set by `guestFileRestore.online.disk.timeout` and `guestFileRestore.restore.files.timeout`.

The default value is "5."

`guestFileRestore.monitorInterval=30`

Specifies the time interval, in minutes, that SnapCenter Plug-in for VMware vSphere monitors for expired guest file restore sessions. Any session that is running beyond the configured session time is disconnected.

The default value is "30."

`guestFileRestore.online.disk.timeout=100`

Specifies the time, in seconds, that SnapCenter Plug-in for VMware vSphere waits for an online disk operation on a guest VM to complete. Note that there is an additional 30-second wait time before the plug-in polls for completion of the online disk operation.

The default value is "100."

`guestFileRestore.restore.files.timeout=3600`

Specifies the time, in seconds, that SnapCenter Plug-in for VMware vSphere waits for a restore files operation on a guest VM to complete. If time is exceeded, the process is ended and the job is marked as failed.

The default value is "3600" (1 hour).

`guestFileRestore.robocopy.directory.flags=/R:0 /W:0 /ZB /CopyAll /EFSRAW /A-:SH /e /NJH /NDL /NP`

Specifies the extra robocopy flags to use when copying directories during guest file restore operations.

Do not remove /NJH or add /NJS because this will break the parsing of the restore output.

Do not allow unlimited retries (by removing the /R flag) because this might cause endless retries for failed copies.

The default values are "/R:0 /W:0 /ZB /CopyAll /EFSRAW /A-:SH /e /NJH /NDL /NP."

`guestFileRestore.robocopy.file.flags=/R:0 /W:0 /ZB /CopyAll /EFSRAW /A-:SH /NJH /NDL /NP`

Specifies the extra robocopy flags to use when copying individual files during guest file restore operations.

Do not remove /NJH or add /NJS because this will break the parsing of the restore output.

Do not allow unlimited retries (by removing the /R flag) because this might cause endless retries for failed copies.

The default values are "/R:0 /W:0 /ZB /CopyAll /EFSRAW /A-:SH /NJH /NDL /NP."

`guestFileRestore.sessionTime=1440`

Specifies the time, in minutes, that SnapCenter Plug-in for VMware vSphere keeps a guest file restore session active.

The default value is "1440" (24 hours).

`guestFileRestore.use.custom.online.disk.script=true`

Specifies whether to use a custom script for onlining disks and retrieving drive letters when creating guest file restore sessions. The script must be located at `[`*`Install Path`*`]\etc\guestFileRestore_onlineDisk.ps1`. A default script is provided with the installation. The values `[Disk_Serial_Number]`, `[Online_Disk_Output]`, and `[Drive_Output]` are replaced in the script during the attach process.

The default value is "false."

`include.esx.initiator.id.from.cluster=true`

Specifies that SnapCenter Plug-in for VMware vSphere should include iSCSI and FCP intiator IDs from all the ESXi hosts in the cluster in the application over VMDK workflows.

The default value is "false."

`max.concurrent.ds.storage.query.count=15`

Specifies the maximum number of concurrent calls that SnapCenter Plug-in for VMware vSphere can make to the SnapCenter Server to discover the storage footprint for the datastores. Plug-in for VMware vSphere makes these calls when you restart the Windows service on the Plug-in for VMware vSphere host.

`nfs.datastore.mount.retry.count=3`

Specifies the maximum number of times SnapCenter Plug-in for VMware vSphere tries to mount a volume as a NFS Datastore in vCenter.

`nfs.datastore.mount.retry.delay=60000`

Specifies the time, in milliseconds, that Plug-in for VMware vSphere waits between attempts to mount a volume as a NFS Datastore in vCenter.

`script.virtual.machine.count.variable.name= VIRTUAL_MACHINES`

Specifies the environmental variable name that contains the virtual machine count. You must define the variable before you execute any user-defined scripts during a backup job. For example, VIRTUAL_MACHINES=2 means that two virtual machines are being backed up.

`script.virtual.machine.info.variable.name=VIRTUAL_MACHINE.%s`

Provides the name of the environmental variable that contains information about the nth virtual machine in the backup. You must set this variable before executing any user defined scripts during a backup.

For example, the environmental variable VIRTUAL_MACHINE.2 provides information about the second virtual machine in the backup.

`script.virtual.machine.info.format= %s|%s|%s|%s|%s`

Provides information about the virtual machine. The format for this information, which is set in the environment variable, is the following: `VM name|VM UUID| VM power state (on|off)|VM snapshot taken (true|false)|IP address(es)`

The following is an example of the information you might provide: `VIRTUAL_MACHINE.2=VM 1|564d6769-f07d-6e3b-68b1-f3c29ba03a9a|POWERED_ON||true|10.0.4.2`

`storage.connection.timeout=600000`

Specifies the amount of time, in milliseconds, that the SnapCenter Server waits for a response from the storage system.

`vmware.esx.ip.kernel.ip.map`

There is no default value. You use this value to map the ESXi IP address to the VMkernel IP address. By default, Plug-in for VMware vSphere uses the management VMkernel adapter IP address of the ESXi host. If you want Plug-in for VMware vSphere to use a different VMkernel adapter IP address, you must provide an override value.

In the following example, the management VMkernel adapter IP address is 10.225.10.56; however, Plug-in for VMware vSphere uses the specified address of 10.225.11.57 and 10.225.11.58. And if the management VMkernel adapter IP address is 10.225.10.60, Plug-in for VMware vSphere uses the address 10.225.11.61.

```
vmware.esx.ip.kernel.ip.map=10.225.10.56:10.225.11.57,10.225.11.5
8; 10.225.10.60:10.225.11.61
```

`vmware.max.concurrent.snapshots=30`

Specifies the maximum number of concurrent VMware snapshots that Plug-in for VMware vSphere performs on the server.

This number is checked on a per datastore basis.

`vmware.max.concurrent.snapshots.delete=30`

Specifies the maximum number of concurrent VMware snapshot delete operations, per datastore, that Plug-in for VMware vSphere performs on the server.

This number is checked on a per datastore basis.

`vmware.query.unresolved.retry.count=10`

Specifies the maximum number of times Plug-in for VMware vSphere retries sending a query about unresolved volumes because of "...time limit for holding off I/O..." errors.

`vmware.quiesce.retry.count=0`

Specifies the maximum number of times Plug-in for VMware vSphere retries sending a query about VMware snapshots because of "...time limit for holding off I/O..." errors during a backup.

`vmware.quiesce.retry.interval=5`

Specifies the amount of time, in seconds, that Plug-in for VMware vSphere waits between sending the queries regarding VMware snapshot "...time limit for holding off I/O..." errors during a backup.

`vmware.query.unresolved.retry.delay= 60000`

Specifies the amount of time, in milliseconds, that Plug-in for VMware vSphere waits between sending the queries regarding unresolved volumes because of "...time limit for holding off I/O..." errors. This error occurs when cloning a VMFS datastore.

`vmware.reconfig.vm.retry.count=10`

Specifies the maximum number of times Plug-in for VMware vSphere retries sending a query about reconfiguring a VM because of "...time limit for holding off I/O..." errors.

`vmware.reconfig.vm.retry.delay=30000`

Specifies the maximum number of time in milliseconds that Plug-in for VMware vSphere waits between sending queries regarding reconfiguring a VM because of "...time limit for holding off I/O..." errors.

`vmware.rescan.hba.retry.count=3`

Specifies the amount of time, in milliseconds, that Plug-in for VMware vSphere waits between sending the queries regarding rescanning the host bus adapter because of "...time limit for holding off I/O..." errors.

`vmware.rescan.hba.retry.delay=30000`

Specifies the maximum number of times Plug-in for VMware vSphere retries requests to rescan the host bus adapter.

Copyright

Trademark

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

doccomments@netapp.com

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

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