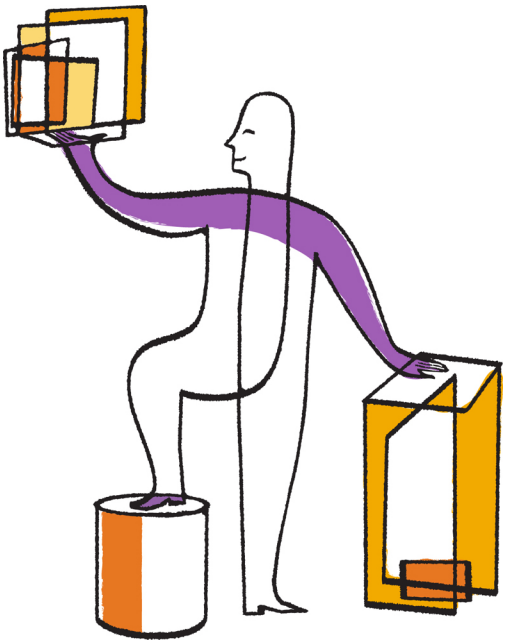
Virtual Storage Console 5.0 for VMware® vSphere®

Installation and Administration Guide



NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089
U.S.

Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 463-8277
Web: www.netapp.com
Feedback: doccomments@netapp.com

Part number: 215-08612_A0
April 2014

Contents

Changes to this document: April 2014

This section contains information about the changes made to this guide for the 5.0 version of Virtual Storage Console for VMware vSphere. Previously, this guide was released with the 4.2.1 version of VSC.

The guide documents the tasks you can perform with VSC. If new information or corrections that affect this guide become available during the VSC release, then this guide is updated with the new information, and this section lists what has changed and when it was changed.

Any time this guide is updated, a note is added to the Release Notes. It is a good practice to check the online Release Notes on a regular basis to determine whether there is new information about using VSC or changes to this guide.

The most current versions of the Release Notes and this guide are located on *NetApp Support*.

April 2014 update

In April 2014, this document was updated to add the following information in support of the 5.0 release of VSC:

- Task instructions have been updated to match the new VSC interface.
  With the move to VMware vSphere Web Client, VSC has changed its interface and the way you access tasks. These changes are reflected throughout the document.
- VSC supports VASA Provider for clustered Data ONTAP.
  Information about installing, registering, and using VASA Provider to create and assign storage capability profiles and threshold alarms has been added.
- Integration with SnapVault after a backup has been added.
  When you add a new backup job, you can specify whether you want to initiate a SnapVault update on the virtual entities that are to be backed up.

In addition, information about features that are no longer supported was removed from the documentation. VSC 5.0 discontinued support for the following:

- vCenter 5.1 and earlier
- VMware Desktop Client
- 32-bit Windows installations
- mbralign
- Single File Restore
- Datastore Remote Replication
- Flash Accel

How to use this guide

This guide has been arranged to make it easy for you to quickly get to the information you need. Many of the changes in this guide are designed to support the new look and content of Virtual Storage Console 5.0 for VMware vSphere, which now integrates with the VMware vSphere Web Client and drops support for the VMware Desktop Client.

The guide is organized into parts based on information that different types of users might need. These include the following broad categories:

- **Conceptional information about VSC, its key components, and how it works with optional plug-ins**
  Target audience: Administrators, executives, and anyone who needs a high-level understanding of how VSC works
  Virtual storage Console for VMware vSphere overview contains this information.
- **What is involved in setting up VSC for your environment**
  Target audience: Administrators
  Plan your VSC for VMware Sphere Virtual storage Console overview provides you with a checklist of issues you should consider before you install VSC. These issues can range from making sure that you have the correct system requirements to whether you want to also install optional features such as VASA Provider for clustered Data ONTAP.
- **Installation and configuration instructions**
  Target audience: Administrators and VSC users
  - *VSC for VMware vSphere installation overview* contains details you need to consider before starting your VSC installation as well as instructions for installing VSC the first time or upgrading an existing version of VSC.
  - *VASA Provider for clustered Data ONTAP installation* provides installation instructions and maintenance information for VASA Provider.
  - *NetApp NFS Plug-in for VAAI installation* tells you how to get that plug-in so that you can use it with VSC.
  - *Configuring your VSC for VMware vSphere environment* provides instructions for configuring ESX server settings, guest operating system timeouts, regenerating VSC SSL certificates, setting up connection brokers, creating storage capability profiles, setting alarms, configuring AutoSupport and email alerts for backup jobs, enabling datastores to be mounted across subnets, and configuring the vCenter Server Heartbeat feature.
- **Role-based access control (RBAC)**
  Target audience: Administrators
  Authentication and user management with vCenter RBAC and Data ONTAP RBAC explains how VSC works with RBAC and describes ways that administrators can manage both vCenter Server and Data ONTAP RBAC when using VSC.
- **Prerequisites for VSC tasks**
  Target audience: Administrators and VSC users

Requirements for performing tasks in VSC for VMware vSphere lists some of the requirements that must be in place before you perform VSC tasks. *Navigating VSC for VMWare vSphere* provides information about how to access tasks within the new VSC GUI.

- **VSC tasks**

  Target audience: Administrators and VSC users

  These sections provide the steps you need to perform to VSC tasks.

  - *Working with storage systems* contains details about the tools VSC provides that enable you to manage storage systems.
  - *Deploying virtual machines on NetApp storage* presents a workflow about provisioning datastores as well as instructions for performing provisioning and cloning operations.
  - *Optimizing performance by aligning the I/O of misaligned virtual machines non-disruptively* contains instructions for tasks that affect checking the alignment of virtual machines and correcting misalignments.
  - *Maintaining your VMware environment* contains tasks such as migrating virtual machines, redeploying virtual machines, reclaiming space from virtual machines, and managing datastores by mounting, resizing, and destroying them.
  - *Backing up virtual machines and datastores* provides tasks that enable you to create and work with backup copies.
  - *Restoring virtual machines and datastores from backup copies* contains the tasks you must perform when you need to restore a backup copy.
- **Troubleshooting**

  Target audience: Administrators and VSC users

  This section identifies possible issues that could affect your VSC installation.
- **Reference**

  Target audience: Administrators and experienced VSC users

  These sections provide information that experienced VSC users might want. This information includes *Provisioning and cloning programmable API*, *Creating customer user accounts for backup and restore operations*, and *VSC CLI commands*.

If you are currently a VSC user, you should check *Changes to this document*, which summarizes some of the key differences from previous releases and how they affect this documentation.

Virtual Storage Console for VMware vSphere overview

Virtual Storage Console for VMware vSphere software is a single vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware environments using NetApp storage systems.

VSC integrates smoothly with the VMware vSphere Web Client and enables you to use Single Sign-on (SSO) services. In addition, the VSC Summary page allows you to quickly check the overall status of your vSphere environment.

Note: The NetApp blue "N" icon in the screens and portlets lets you easily distinguish the NetApp features from the VMware ones.

By running VSC, you can perform tasks such as:

- **Manage storage and configure the ESX host**
  You can use VSC to add, remove, assign credentials, and set up permissions for storage controllers within your VMware environment. In addition, you can manage ESX and ESXi servers connected to NetApp storage. You can set values for host timeouts, NAS, and multipathing as well as view storage details and collect diagnostic information.

  Note: You can also add Storage Virtual Machines (SVMs, formerly known as Vservers).
- **Create storage capability profiles and set alarms**
  When you install a VASA Provider for clustered Data ONTAP and register it with VSC, you gain access to storage capability profiles and the ability to set alarms to warn you when the thresholds for volumes and aggregates are approaching full.
- **Provision datastores and clone virtual machines**
  VSC uses FlexClone technology to let you efficiently create, deploy, and manage the lifecycle of virtual machines from an interface that has been integrated into the VMware environment.
- **Perform online alignments and migrate virtual machines singularly and in groups into new or existing datastores**
  You can use VSC to quickly check the alignment status of virtual machines. If there are alignment issues with the virtual machines, you can, in most cases, resolve those issues without having to power down the virtual machines.
- **Back up and restore virtual machines and datastores**
  VSC allows you to rapidly back up and restore virtual entities such as virtual machines or datastores on NetApp storage.

To provide security while performing tasks, VSC supports role-based access control (RBAC) at two levels:

- vSphere objects, such as virtual machines and datastores.
  These objects are managed using vCenter RBAC.
- Data ONTAP storage

Storage systems are managed using Data ONTAP RBAC.

If access control is not an issue, you can log in as administrator and have access to all the features that VSC provides.

Tip: The View privilege is required for all users who do not have administrator privileges. Without this privilege, these users cannot see the VSC GUI.

As a vCenter Server plug-in, VSC is available to all vSphere Clients that connect to the vCenter Server. Unlike a client-side plug-in that must be installed on every vSphere Client, you install the VSC software on a Windows server in your data center.

Related concepts

VASA Provider for clustered Data ONTAP and VSC for VMware vSphere on page 14
Provisioning and cloning datastores and virtual machines on page 16
How VSC for VMware vSphere optimizes I/O performance of misaligned virtual machines on page 17
Backing up and restoring virtual machines and datastores on page 18
Authentication and user management with vCenter RBAC and Data ONTAP RBAC on page 81

How VSC for VMware features work with optional plug-ins

Virtual Storage Console for VMware vSphere supports optional plug-ins and virtual appliances that work with VSC features. You can enhance your experience with VSC by installing NFS Plug-in for VAAI and VASA Provider for clustered Data ONTAP.

Note: The installation package for NFS Plug-in for VAAI is not included in the VSC software download package. The VASA Provider installation software is available for download from the Virtual Storage Console 5.0 for VMware vSphere Download page and from the VASA Provider for Clustered Data ONTAP Download page, which are available on the NetApp Support Site.

NetApp Support

VSC cloning and provisioning operations benefit from the NFS Plug-in for VMware VAAI. The plug-in integrates with VMware Virtual Disk Libraries to provide VMware vStorage APIs for Array Integration (VAAI) features, including copy offload and space reservations. These features can improve the performance of cloning operations because they do not need to go through the ESXi host.

VASA Provider is a virtual appliance that improves storage management. It provides information to the vCenter Server about the NetApp storage systems being used in the VMware environment. Integrating with the vCenter Server this way enables you to make more informed decisions. For example, you can create storage capability profiles that define different storage Service Level Objectives (SLOs) for your environment. You can then use these SLOs to select a datastore with the right storage attributes when provisioning virtual machines. In addition, you can set up alarms to

notify you when a volume or aggregate is nearing full capacity or a datastore is no longer in compliance with its associated SLO.

VASA Provider for clustered Data ONTAP and VSC for VMware vSphere

VASA Provider for clustered Data ONTAP uses VMware VASA (vSphere APIs for Storage Awareness) to provide better storage management. By providing information about storage used by Virtual Storage Console for VMware vSphere to the vCenter Server, VASA Provider both enables you to make more intelligent virtual machine provisioning decisions and allows the vCenter Server to warn you when certain storage conditions may impact your VMware environment.

You can use VASA Provider to set up storage capability profiles that define Service Level Objectives (SLOs) and associate them with different storage capabilities, such as disk type, high availability, disaster recovery, performance features, deduplication, and space efficiency. You can assign the profiles to datastores whose attributes match the profile. Then, when you need to provision virtual machines, you can easily select datastores that best match the storage requirements of the virtual machines that you are creating. In addition, VASA Provider enables you to define and maintain consistency in your storage SLOs.

VASA Provider continuously monitors these datastores for compliance with the associated profiles. If the attributes associated with a datastore change and cause it to fall out of compliance, VASA Provider displays an alarm.

By default, VASA Provider provides three standard storage capability templates. Companies have different storage environments. You can use these templates as the basis to create the appropriate profiles for your storage environment. VASA Provider is shipped with the following templates:

Template	**Storage SLO**
Gold-Template	The Gold template targets the needs of business critical storage. It has the following features: • Very high performance • Performance isolation • Disaster recovery isolation • Long retention of the storage
Silver-Template	The Silver template targets the needs of departmental storage. It has the following features: • High performance • Performance isolation • Disaster recovery on a group • Short retention of the storage

Template	Storage SLO
Bronze-Template	The Bronze template supports other applications. It has the following features: • High capacity • Performance limits on the group • No disaster recovery • No retention

To view the settings for these templates, select the template on the Storage Capability Profile page and view its Summary page.

You can create your own profiles by using one of the following methods:

- Create a new profile from scratch.
- Clone an existing profile, such as one of the templates, and edit it to meet your SLO needs.
- Reverse engineer a profile by running Auto-generate on an existing datastore.

When you use VSC's provisioning features, you can specify a storage capability profile, and the provisioning wizard then creates storage to match those storage capabilities. This enables you to quickly provide a consistent template that has all the necessary resources for the tasks associated with the storage.

In addition, you can manually map a profile to any datastore that has resources matching that profile.

Related tasks

Registering VASA Provider for clustered Data ONTAP with VSC for VMware vSphere on page 64
Creating and editing storage capability profiles on page 65

Alarm options available with VASA Provider

The alarm features of VASA Provider for clustered Data ONTAP enable you to monitor both how close a volume or aggregate is to reaching full capacity and whether a datastore is in compliance with its associated profile.

To monitor the volume or aggregate capacity, you can set threshold limits on the VASA Provider Settings page. Aggregate level alarms affect all volumes in the aggregate. Volume level alarms affect all LUNs in the volume.

VASA Provider displays a yellow alarm if the volume or aggregate reaches the "Nearly full" percent and a red alarm if it reaches the "Full" percent. The default values for the threshold alarms are 80% for nearly full and 90% for full.

VASA Provider checks these values every 15 minutes. If you need to check these values sooner, you can select the **Check Compliance** button on the Storage Mapping page.

In addition to threshold alarms, VASA Provider continuously checks whether a datastore is compliant with its storage capability profile. This checking is automatic; you do not need to set it up.

Datastores can fall out of compliance as a datacenter evolves and you move volumes, expand clusters, or perform other work with datacenters that affects the capabilities associated with the datastore profile. VASA Provider displays a yellow alarm when it discovers a datastore that is no longer compliant with its associated profile. If you fix the issue, the web client might continue to display the alarm as yellow.

Note: VASA Provider only displays compliance alarms if the threshold status is green for both volumes and aggregates.

If two alarms are triggered at the same time, you must manually clear both alarms.

Related tasks

Setting alarm thresholds in VASA Provider for clustered Data ONTAP on page 69

Provisioning and cloning datastores and virtual machines

Virtual Storage Console for VMware vSphere enables you to provision datastores and quickly create multiple clones of virtual machines in the VMware environment.

VSC's Create Rapid Clones wizard lets you create multiple clones from one virtual machine template. Cloning from a template saves time and enables you to set up virtual machines that all have the same configuration.

If you have VASA Provider for clustered Data ONTAP installed, you can use existing storage capabilty profiles to ensure that the new storage is configured consistently.

You can also use connection brokers, such as VMware View Server or Citrix XenDesktop, to import virtual machines into a virtual desktop infrastructure.

In addition, it is a good practice to have the NFS Plug-in for VMware VAAI installed before you perform provisioning and cloning operations. The plug-in can improve performance during the operations.

Note: VSC does not support IPv6. If you have IPv6 configured on a LIF, VSC cannot use any Storage Virtual Machines (SVMs, formerly known as Vservers) from that cluster.

Related concepts

Deploying virtual machines on NetApp storage on page 112

Related tasks

Provisioning datastores on page 113

How VSC for VMware vSphere optimizes I/O performance of misaligned virtual machines

Virtual Storage Console for VMware vSphere provides a non-disruptive, interim solution for the performance penalty introduced by misaligned virtual machines. Rather than align the misaligned VMDKs, which requires downtime, VSC aligns the I/O without requiring downtime by offsetting the VMDKs within optimized datastores.

A virtual machine is misaligned when VMDK partitions do not align with the block boundaries of the storage system. As a result, the storage system might read or write to twice as many blocks of storage than is necessary.

VSC can scan datastores to determine which virtual machines are misaligned and, if possible, perform an online alignment by non-disruptively migrating the misaligned virtual machines to a datastore that is optimized for the VMDK layout. VSC optimizes the datastore by functionally aligning I/O to the offset of the largest partition.

Online alignment is a good choice for virtual machines that you cannot take offline. When possible, you should take the virtual machine offline and physically align the VMDK using a tool such as VMware vCenter Converter.

Methods for migrating virtual machines

Virtual Storage Console for VMware vSphere provides two options for virtual machine migration: optimizing I/O performance for a misaligned virtual machine and moving virtual machines from one datastore to another.

Goal	**What the migration does**	**Location in the vSphere Web Client**
Align I/O of misaligned virtual machines non-disruptively	Performs an online alignment by non-disruptively migrating the misaligned virtual machines to a datastore that is optimized for the VMDK layout.	**Virtual Storage Console > Optimization and Migration**

Goal	What the migration does	Location in the vSphere Web Client
Migrate virtual machines to another datastore	Migrates virtual machines to a new or existing datastore. **Note:** If the selected virtual machines do not have the same offset group, the target datastore will not be optimized for all virtual machines. VSC creates a datastore optimized for the offset group of the last virtual machine that it migrates.	**vCenter > Inventory Lists > Virtual Machines**

Related tasks

Optimizing performance by aligning the I/O of misaligned virtual machines non-disruptively on page 122
Migrating virtual machines to a new or existing datastore on page 129

Backing up and restoring virtual machines and datastores

Virtual Storage Console for VMware vSphere provides backup and restore features that enable you to create backup copies of virtual machines and datastores and later restore them.

To use these features, you must select the **Backup and Recovery** option included in the VSC installation program. Unlike other VSC features, the backup and restore features require that you have an SMVI license.

Note: The VSC GUI displays the backup and restore interface even if you have not installed it or purchased the SMVI license. But, if you attempt to perform a backup, restore, mount, or unmount operation, you receive an error message.

The VSC backup feature provides you with several options, including the following:

- Using SnapMirror or SnapVault when performing backups
- Performing a one-time, on-demand backup
- Scheduling backups to occur on a regular basis
- Specifying a retention policy for the backups
- Adding a virtual machine or datastore to an existing backup
- Modifying the job properties of an existing backup

You can restore a backup copy whenever you need to. VSC enables you to restore a datastore, an entire virtual machine, or particular disks from a virtual machine. To confirm that the backup copy is correct, you can mount the backup copy to a different host, verify the backup contents, unmount the backup from that host, and then restore the backup copy to the original location.

Related concepts

Backing up virtual machines and datastores on page 138

VSC for VMware vSphere protects system resources by using lock management

Virtual Storage Console for VMware vSphere uses lock management to avoid having simultaneous tasks performed on the same target datastores or virtual machines . As a result, certain alignment, migration, provisioning or cloning, and backup and recovery features that could impact each other become temporarily unavailable if another task is being performed on the target datastore or virtual machine.

For example, if you are migrating virtual machines, you cannot clone one of the virtual machines until the migration operation completes. Or, if you provisioning storage, you cannot perform the following backup or restore operations on the target datastore or virtual machine until the provisioning operation completes:

- Create on-demand backup copies of individual virtual machines, datastores, or a datacenter.
- Schedule automated backup copies of individual virtual machines, datastores, or a datacenter.
- Recover a datastore, virtual machine, or virtual disk file.
- Mount a backup for a file restore session.
- Unmount a backup that was previously mounted for a file restore session.

  Note: When a lock occurs during a mount or unmount operation for a file restore session, the lock is held from when the backup is mounted to the virtual machine until the backup is unmounted.

Before you start an operation, it is a good practice to make sure the target datastore or virtual machine is not being used by another operation.

VSC for VMware vSphere architecture

The Virtual Storage Console for VMware vSphere architecture includes the storage system running Data ONTAP, the vCenter Server, the VMware vSphere Web client, and the ESX and ESXi hosts.

VSC uses VMware-recommended web-based architecture. It consists of two major components:

- A graphical user interface (GUI) web application that displays as a plug-in within the vSphere Web client to provide a single management console for virtualized environments.
- A server component that is controlled by the VSC service and hosts Java Servlets to handle the GUI and API calls to and from the storage systems and the ESX and ESXi hosts.

When you run VSC, you use the VMware Web vSphere client and the VMware vCenter server. VSC provides the following:

- A single VSC plug-in with one user interface and help file.
- The VSC server
- The SMVI server

You can also can write applications that communicate with the VSC server. For example, you can use the SOAP API to create an application. VSC supports the Provisioning and Cloning API.

The vSphere client and any applications you create use the HTTPS protocol to communicate. The VSC server and the SMVI server use ZAPI to communicate with the storage systems that are running Data ONTAP. Communication from the VSC server to the vCenter is done using SOAP.

The vCenter server communicates with the physical servers where ESX or ESXi hosts are running. You can have multiple virtual machines running on the ESX or ESXi hosts. Each virtual machine can run an operating system and applications. The ESX and ESXi hosts then communicate with the storage systems.

Plan your VSC for VMware vSphere installation

Before you install Virtual Storage Console for VMware vSphere, it is a good practice to plan your installation and decide how you want to configure your VSC environment, including whether you want to install other plug-ins or virutal appliances that work with VSC, such as NFS Plug-in for VAAI or VASA Provider.

The following is a high-level overview of what you need to consider when you install and configure VSC:

Consider...	**Explanation...**
What are the requirements for installing VSC?	You must install the VSC software on a 64-bit Windows server with at least 4 GB of RAM. Do not install it on a client computer. Also, the vCenter Server must be running vSphere 5.5. In addition, some of the VSC features use products that require you purchase a software license. **More information:** • Interoperability Matrix, which is available online at *support.netapp.com/matrix* • *Installation overview* on page 26 • *VSC for VMware vSphere supported configurations* on page 57

Consider...	**Explanation...**
What sort of role-based access control (RBAC) do you need?	VSC supports both vCenter Server RBAC and Data ONTAP RBAC. If you plan to run VSC as an administrator, you will have all the necessary permissions and privileges for all the tasks. If your company requires that you restrict access to vSphere objects, you can assign users to the standard VSC roles to meet the vCenter Server requirements. You can create the recommended Data ONTAP roles using the "RBAC User Creator for Data ONTAP" tool, which is available on the NetApp ToolChest. If a user attempts to perform a task without the correct privileges and permissions, the task options are grayed out. **More information:** • *Installation overview* on page 26 • *Standard roles packaged with VSC for VMware vSphere* on page 87 • *Recommended Data ONTAP roles when using VSC for VMware vSphere* on page 92 • *Authentication and user management with vCenter RBAC and Data ONTAP RBAC* on page 81

Consider...	**Explanation...**
Is this the first time you have installed VSC or is this an upgrade?	**(Initial installation)** The VSC installation wizard automatically installs most of the VSC features, but it gives you the option of installing backup and restore features. You can also install these features later. **More information:** • *Installing VSC for VMware vSphere using the installation wizard* on page 29 • *Installing VSC for VMware vSphere using silent mode* on page 30 **(Upgrade installation)** You can only upgrade to the following: • 64-bit Windows systems • vSphere 5.5 environments Best practices before an upgrade include the following: • Record information about the storage systems being used and their credentials, especially those storage systems being used for backup and restore operations. After the upgrade, verify that all the storage systems were automatically discovered and they have the correct credentials. • If you modified any of the standard VSC roles, you should clone those roles in order to save your changes. VSC overwrites the standard roles with the current defaults each time you restart the VSC service. • If you made any changes to the VSC preferences file, you should record those changes. Each time you install VSC, it overwrites the current preferences files. **More information:** • *Upgrade installation of VSC for VMware vSphere* on page 32 • *Performing a standard VSC for VMware vSphere upgrade installation* on page 34 • *Upgrading from a 32-bit installation to a 64-bit installation of VSC 5.0 for VMware vSphere* on page 35
Have you registered your VSC installation?	After you install VSC, you must register it with the vCenter Server. **More information:** • *Registering VSC for VMware vSphere with vCenter Server* on page 58

Consider...	Explanation...
Are your ports set up correctly for VSC?	VSC uses designated ports to enable communication between its components. If you have firewalls enabled, you might need to manually grant access to specific ports for VSC. **More information:** • *VSC for VMware vSphere port requirements* on page 61
Do you need to regenerate an SSL certificate for VSC?	The SSL certificate is automatically generated when you install VSC. You might need to regenerate it to create a site-specific certificate. **More information:** • *Regenerating an SSL certificate for VSC* on page 58
Were your ESX server values set correctly?	While most of your ESX server values are set by default, it is a good practice to verify them. **More information:** • *ESX server and guest operating system setup* on page 49
Do you need to set up the guest operating system timeout values?	The guest operating system (GOS) timeout scripts set the SCSI I/O timeout values for supported Linux, Solaris, and Windows guest operating systems to ensure correct failover behavior. **More information:** • *Timeout values for guest operating systems* on page 53
Will you be performing provisioning and cloning tasks using connection brokers?	You can add connection brokers to your system and use them to import virtual machines into a virtual desktop infrastructure. **More information:** • *Managing connection brokers* on page 61
Do you plan to use storage capability profiles?	To use storage capability profiles, you must install VASA Provider. **More information:** • *Installing VASA Provider for clustered Data ONTAP* on page 40 • *Registering the VASA Provider for clustered Data ONTAP with VSC for VMware vSphere* on page 64 • *Creating and editing storage capability profiles* on page 65 • *Mapping storage associated with VASA Provider for clustered Data ONTAP* on page 71 • *Setting alarm thresholds* on page 69

Consider...	**Explanation...**
Do you plan to use NFS Plug-in for VAAI?	The plug-in provides VAAI features, such as copy offload and space reservations, which can improve the performance some provisioning and cloning operations. **More information:** • *NFS Plug-in for VAAI installation* on page 48

VSC for VMware vSphere installation overview

While the basic installation of the Virtual Storage Console for VMware vSphere software is simple, installation does require that you consider things such as whether you have a 64-bit Windows server, if you want to install the backup and restore features, whether you need a special software license, and if you going to need to set up RBAC.

Installation guidelines

To install VSC, you must have 64-bit Windows server and the vCenter Server must be running vSphere 5.5. For information about which versions of Windows and other features are supported, see the Interoperability Matrix, which is available online at *support.netapp.com/matrix*.

Note: Do not install this software on a client computer.

The following are some guidelines for installing the VSC software:

- VSC must be installed on a local disk of the Windows server. Do not attempt to install VSC on a network share.
- The network must be connected between the Windows server running VSC and the management ports of the storage controllers, the ESX/ESXi hosts, and the vCenter Server.
- A reboot is not required to complete the installation. However, vSphere clients must be closed and restarted to be able to display the VSC plug-in.
- At a minimum, the display must be set to 1,280 by 1,024 pixels to view VSC pages correctly.

Backup and restore features require manual selection during installation

VSC automatically installs the software modules to support all its features except the backup and restore features. You must purchase a license for SnapManager for Virtual Infrastructure in order to perform backup and restore operations. As a result, VSC requires that you explicitly select the backup and restore features in the VSC installation menu.

The VSC GUI displays information about the backup and restore options regardless of whether you installed those features. However, if you attempt to perform a backup, restore, mount, or unmount operation, you will receive an error message. You can only perform those operations when the software supporting the backup and restore features is installed.

Software licenses that might be needed

The following software licenses might be required for VSC depending on which features you use:

- The required protocol license (NFS, FCP, iSCSI)
- SnapManager for Virtual Infrastructure (if performing backup and restore operations)
- SnapMirror (required for the provisioning and cloning template distribution feature and for the backup SnapMirror update option)

- SnapRestore (if performing backup and restore operations)
- A_SIS (if using provisioning and cloning features when configuring deduplication settings)
- MultiStore (if using provisioning and cloning features and working with vFiler units)
- FlexClone
  The FlexClone license is required in the following situations:
  - You are using VSC to clone virtual machines.
  - You are performing backup and restore operations in NFS environments and running a version of Data ONTAP prior to 8.1.

You do not need a FlexClone license if you are performing backup and restore operations in NFS environments with one of the following versions of Data ONTAP:

- Data ONTAP 8.1 operating in 7-Mode
- Clustered Data ONTAP 8.1.1 or later

RBAC access to VSC required for users

VSC supports vCenter Server and Data ONTAP role-based access control (RBAC). As a result you must provide users with the appropriate RBAC permissions. The vCenter Server permissions determine whether a user has or does not have access to certain VSC tasks for certain vSphere objects.The Data ONTAP privileges provide the credentials used by the storage systems.

To simplify the process of creating vCenter Server user roles, VSC provides several standard VSC roles for key tasks. These roles contain all the VSC-specific and native vCenter Server privileges required for the tasks. As administrator, you can assign these roles to users.

Note: You should not edit the standard roles that VSC provides. These roles return to their default settings each time you restart the VSC service. This means that any changes you made to these roles will be lost if you modify or upgrade your installation. If you need a privilege that these roles do not provide, you can create a role containing that privilege and then use the Groups feature to combine that role with the appropriate standard VSC role. Or you can clone the standard VSC role and then modify the cloned role to meet your needs.

Unless your company's security policies require more restrictive permissions, it is a good practice to assign permissions on the root object (also referred to as the root folder). Then, if you need to, you can restrict those entities that you do not want to have permissions.

All VSC users must have the View privilege correctly assigned

The VSC-specific View privilege is read-only and enables users to see the menus, tabs, and other elements of the VSC interface. This privilege must be included in all VSC roles, or the user will not be to view the VSC interface.

If you want to provide a user with read-only access to VSC, you can assign the user the standard VSC Read-only role, which includes the View privilege.

It is a good practice to assign the permission containing this privilege to the root object.

Confirm that the storage systems and their credentials are available

VSC provides centralized management for storage discovery and credentials. All VSC features use the credentials entered during the initial setup and discovery process.

If you are upgrading from VSC 4.1 or earlier, you should check the storage systems to ensure that there are not issues with credentials, especially with regard to backup and recovery operations, after you install the backup and restore features.

Make sure the times are synchronized when installing VSC on a different server

If you are not installing VSC on the vCenter Server, you must make sure that the times on the VSC installation server and the vCenter Server are synchronized.

The vCenter Server will not accept the certificate of the VSC installation server when the times differ on the servers.

For information on synchronizing the server times, see your operating system documentation.

VSC for VMware vSphere supported configurations

Virtual Storage Console for VMware vSphere requires the VMware vSphere Web Client and is supported on specific releases of ESX/ESXi, vSphere, and Data ONTAP software. See the Interoperability Matrix, which is online at *support.netapp.com/matrix*, for details.

vSphere server configuration

VSC requires that you have vCenter Server 5.5.

If you are installing VSC on a vCenter Server that has a large number of ESX/ESXi hosts, make sure that there is sufficient CPU and memory resources to support VSC in your environment. If the vCenter Server is consuming all the resources to manage the hosts, the VSC service will not be able to respond to the requests it receives. The amount of resources needed varies based on your system setup.

Windows server configuration

Your Windows system must meet minimum hardware requirements before installing the VSC software.

The memory requirements depend on whether you install VSC on the same machine as the vCenter Server or on a different machine. When this document was created, the memory requirements for 64-bit environments where VSC was installed on a separate machine were the following:

- Minimum memory requirement: 4 GB RAM
- Recommended memory requirement: 4 GB RAM

Hardware requirements are higher if you are running VSC on the same machine as the vCenter Server.

Note: Please refer to VMware documentation for the current list of hardware requirements.

You should be aware of the following requirements before you install the VSC software:

- Supported Microsoft Windows software
- vCenter Server requirements
- ESX host software requirements
- Data ONTAP requirements

Note: IPv6 is not supported on VSC. If the server on which you are installing VSC has IPv6 enabled, you should disable IPv6 before installing VSC. IPv6 should not be re-enabled after VSC is installed.

VMware vSphere Web Client configuration

The client computer that runs the vSphere Web Client software must have a web browser installed.

VSC supports all browsers that the vSphere Web Client supports.

VSC only supports having the vSphere Web Client attached to one vCenter Server; it cannot be connected to multiple vCenter Servers.

Initial installation of VSC for VMware vSphere

If this is the first time you are installing Virtual Storage Console for VMware vSphere, you do not need to worry about upgrade issues. You can install VSC using either the installation wizard or silent mode.

The wizard steps you through the process and gives you the option of installing the backup and restore features. It installs the rest of the VSC features by default. Because the backup and restore features require the purchase of a SnapManager for Virtual Infrastructure license, some people choose not to install those features.

If you use silent mode to install VSC, you must enter a command line telling VSC which options to install.

Installing VSC for VMware vSphere using the installation wizard

You can use the installation wizard to install Virtual Storage Console for VMware vSphere. By default, the VSC software installs all the features except the backup and restore features. You must manually select the option to install those features because they normally require that you purchase a license for SnapManager for Virtual Infrastructure.

Before you begin

- You must log in with administrator privileges for the machine on which you install VSC.
- You can only install VSC on a 64-bit Windows server.

- Before you install VSC, verify that your system meets the VSC requirements listed in the Interoperability Matrix, which is available online at *support.netapp.com/matrix*.

Steps

1. Download the VSC installer.
2. Double-click the installer icon, and click **Run** to start the installation wizard.
3. Follow the instructions in the installation wizard to install the software.

   Note: If you want to install backup and restore features, you must select that option. Otherwise, the VSC installer does not install it. Menu options for the features will appear in the installed VSC GUI, but you will not be able to use them.
4. Click **Finish** to complete the installation.
5. At the web page that appears after the installation completes, register VSC with the vCenter Server.

   You must provide the vCenter Server host name or IP address and the administrative credentials.

   Note: To register VSC with the vCenter Server, you must have administrator privileges for your Windows login.

Installing VSC for VMware vSphere using silent mode

You can install Virtual Storage Console for VMware vSphere using silent mode instead of the installation wizard. When you use silent mode, you enter a command line that lets you automatically install all the VSC features at one time.

Before you begin

- You must log on with administrator privileges for the machine on which you install VSC.
- You can only install VSC on a 64-bit Windows server.
- Before you install VSC, verify that your system meets the VSC requirements listed in the Interoperability Matrix, which is available online at *support.netapp.com/matrix*.

Steps

1. Download the VSC installer.
2. Use the following command format to install VSC:

   ***installer.exe* /s /v"/qn /Li *logfile*ADDLOCAL=ALL INSTALLDIR=\"*installation path*\""**

   This command installs all the VSC features, including the backup and restore features.

Example

The following is a sample command line for a 64-bit host machine:

```
VSC-5.0-win64.exe /s /v"/qn /Li install.log ADDLOCAL=ALL INSTALLDIR=\"C:
\Program Files\NetApp\Virtual Storage Console\""
```

3. At the web page that appears when the installation is complete, register VSC with the vCenter Server.

   You must provide the vCenter Server host name or IP address and the administrative credentials.

   Note: To register VSC with the vCenter Server, you must have administrator privileges for your Windows login.

Installing or uninstalling the VSC backup and restore features

The installation wizard lets you install or uninstall the Virtual Storage Console for VMware vSphere backup and restore features separately. The other VSC features can be installed or uninstalled only as a group. You can install or uninstall the backup and restore features with the other features or at a different time.

About this task

The steps that follow describe how to install the backup and restore features after you have already installed the other features.

You can also use this backup and restore check box to uninstall only those features. It has no effect on the other installed VSC features.

Steps

1. On the Windows server where you installed the VSC software, go to the **Control Panel** and select the option for your version of Windows that lets you add programs.

   For example, if you are running Windows Server 2003, you would choose **Control Panel** > **Add/Remove Programs**, but for Windows 2008, you would choose **Control Panel** > **Programs and Features**.

2. Select **VSC for VMware vSphere** and click **Change** to start the installation wizard.
3. In the installation wizard, select the **Modify** option and click **Next**.
4. Select the check box for the backup and restore features if you want to add them, or clear the check box if you want to remove them, and click **Next**.
5. If you are installing the backup and restore features, click **Install** to start the installation.
6. Click **Finish** to complete the installation or the removal of these features.

After you finish

You must close the vSphere Client and restart it to activate the new features.

The VSC interface displays the menu options for the backup and restore features even if they are not installed; however, you can only use these menu options if the features are installed.

If you install the backup and restore features separately from the other features, you must restart the VSC service after the installation completes.

Upgrade installation of VSC for VMware vSphere

If you are running a 4.x version of Virtual Storage Console for VMware vSphere, you can perform an upgrade installation as long as your environment meets the VSC requirements. Before you upgrade, make a record of the information that VSC does not update and the storage systems in use. Also, if you are using VASA Provider for clustered Data ONTAP, you must unregister it.

Check for changes to VSC requirements

Unlike previous versions, VSC 5.0 only works with 64-bit Windows servers. If you are currently running in a 32-bit Windows environment, you must perform special steps and manually move certain data in order to upgrade to a 64-bit Windows system. For information on doing this, see *Upgrading from a 32-bit installation to a 64-bit installation of VSC 5.0 for VMware vSphere* on page 35.

In addition, VSC 5.0 requires that the vCenter Server be running vSphere 5.5. If you attempt to install VSC 5.0 on an earlier version of vSphere, you will receive an error message. This message varies depending on whether you have thick provisioning enabled. With thick provisioning the message is similar to the following:

```
The VSC plugin is only available in the vSphere web
client.
```

Without it, the error message is the following:

```
Registration failed with the following message:
NVPF-00017: This version of vCenter (5.1.0) found at
https://00.00.000.000:443/sdk is not supported. Please upgrade
to vCenter 5.5 or later.
```

For complete information about the VSC requirements, see the Interoperability Matrix, which is available online at *support.netapp.com/matrix*.

Record storage system information

VSC automatically rediscovers your storage after you perform an upgrade. It is a good practice to record your storage system information before the upgrade so that you can confirm that all the storage systems were rediscovered after the upgrade.

If you are using backup and restore features, it is important to record the storage systems used for those operations and the credentials associated with them. Prior to VSC 4.2 for VMware vSphere, the Backup and Recovery plug-in managed its own storage system discovery and credentials. Because

VSC did not discover those storage systems, they might not appear in the list of storage systems that VSC manages.

After an upgrade, when you check the storage systems used for backup and restore operations, you should also verify that they have at least the minimum credentials required to perform these operations. You can use VSC to update the credentials.

If any storage systems are missing after the upgrade, you can select the **Update All** icon to force VSC to discover storage systems. If that does not work, you can manually add the storage system using VSC's **Add** icon or vCenter's **Add storage system** option in the Actions menu.

Note: If the storage system does not have storage mapped to an ESX/ESXi host that a vCenter Server is managing, VSC does not automatically discover it.

Record any changes you made to standard VSC roles

You should not modify the VSC standard roles. If you make changes to these roles, you will lose those changes when you upgrade your VSC installation or restart the VSC Windows service. These roles return to the current default values each time you install VSC, restart the VSC Windows service, or modify your VSC installation.

If you made any changes to these roles, you should record the changes. After you upgrade your installation, you can create new roles that have those changes.

Note: Instead of editing the standard VSC roles, you should clone them and then edit the cloned roles.

Record any changes you made to the preferences file

The upgrade process overwrites the existing preferences files with new preferences files for features that VSC uses. It is a good practice to record changes you made to preference files before an upgrade.

For provisioning and cloning tasks, VSC creates a backup of the preferences file, `etc/kamino/old_kaminoprefs.xml`. If you had modified the `etc/kamino/kaminoprefs.xml` preferences file, you can copy the changes from `etc/kamino/old_kaminoprefs.xml` to the new file that VSC creates during the update.

Unregister VASA Provider

If you are using VASA Provider, you must unregister it before you upgrade your VSC software. If you do not unregister it, you might not be able to see the VASA Provider GUI when you register it in the upgraded installation.

Performing a standard VSC for VMware vSphere upgrade installation

If you currently have version 4.x of Virtual Storage Console for VMware vSphere installed, you can upgrade VSC. The VSC installer checks the version numbers of each of the currently installed VSC component to determine whether you are upgrading to a newer version.

Before you begin

The VSC installer automatically upgrades all the installed VSC features to the newer versions. If you do not have backup and restore features installed, the VSC installer gives you the option of installing them.

The VSC installer does not support upgrades from the following:

- VSC 2.1.2 or earlier
- A standalone version of Rapid Cloning Utility (RCU)
- A standalone version of SnapManager for Virtual Infrastructure (SMVI)

If you have any of that software installed, you must uninstall it before you can install the current version of VSC. If the VSC installer finds RCU, or SMVI on the server, it prompts you to uninstall the software, and then aborts. It also aborts if you have VSC 1.x installed.

You must be logged on with administrator privileges to the machine where you installing VSC.

Important: If you are using VASA Provider for clustered Data ONTAP, unregister it from VSC before you install the upgrade.

Steps

1. Download the installer for VSC.
2. Double-click the installer icon, and click **Run** to start the installation wizard.
3. Click **Yes** on the confirmation prompt.
4. Review your installation options.

   The installation wizard gives you the option to select the backup and restore features if they are not currently installed.
5. Click **Next** to start the installation.

   The wizard automatically selects all currently installed features and upgrades them.

   The installation might take several minutes.
6. Click **Finish** to complete the installation.
7. At the web page that appears when the installation is complete, register VSC with the vCenter Server.

   You must provide the vCenter Server host name or IP address and the administrative credentials.

Note: To register VSC with the vCenter Server, you must have administrator privileges for your Windows login.

Upgrading VSC for VMware vSphere from a 32-bit installation to a 64-bit installation

If you are currently running Virtual Storage Console 4.x for VMware vSphere on a 32-bit Windows platform, you can upgrade to VSC 5.0, which requires a 64-bit platform. Going to a 64-bit platform requires that you manually move directories from the 4.x installation to the 5.0 installation in addition to performing the standard upgrade procedures.

Before you begin

You must have administrator privileges on the system where you are installing VSC.

You should always check the Interoperability Matrix, which is online at *support.netapp.com/matrix*, to confirm that you system meets the requirements for VSC.

Steps

1. Download the VSC software package.
2. **(VSC 4.x system)** Stop the VSC Windows service.

   If you have been using the backup and restore features, make sure that you also stop the SnapManager for Virtual l Infrastructure (SMVI) service.
3. **(VSC 4.x system)** Copy the following VSC 4.x directories and files.

   Note: To make moving these files to your VSC 5.0 installation easier, you can create a .zip file to contain them.

   These directories and files are all relative to the VSC installation directory.

   - `etc\keystore.properties`
   - `etc\nvpf.keystore`
   - `etc\nvpf.override`
   - `etc\network-interface.properties`
   - `etc\caster\casterprefs.xml`
   - `etc\caster\derby\`
   - `etc\caster\kaminosdkprefs.xml`
   - `etc\kamino\baselines.ser`
   - `etc\kamino\connectionBrokers.ser`
   - `etc\kamino\vcenters.ser`
   - `etc\kamino\kaminoprefs.xml`
   - `etc\vsc\vsc.xml`
   - `etc\vsc\vscPreferences.xml`
   - `log\`

- `smvi\server\etc\cred`
- `smvi\server\etc\keystore`
- `smvi\server\etc\smvi.keystore`
- `smvi\server\repository\`

4. **(VSC 5.0 system)** Run the VSC 5.0 installation program.

   This program automatically installs most VSC features. If you want to use the VSC backup and restore features, you must manually select that option. The backup and restore features require the SMVI license.

   See the section "Software licenses" for more information about licenses that you might need in order to use VSC.

5. **(VSC 5.0 system)** Register VSC with the vCenter Server when the registration web page opens.

   For details about how to register VSC or what to do if the registration web page does not open, see the section "Registering VSC for VMware vSphere with vCenter Server."

6. **(VSC 5.0 system)** Stop the VSC Windows service.

7. **(VSC 5.0 system)** Place the VSC 4.x files into your VSC 5.0 installation.

   If you created a .zip file to contain these directories and files, you need to paste it into the VSC 5.0 installation directory and then unzip it.

   You should paste these files relative to the VSC 5.0 installation directory.

8. **(VSC 5.0 system)** Restart the VSC Windows service.

9. **(VSC 5.0 system)** Re-register VSC with the vCenter Server.

10. **(VSC 5.0 system)** Verify that the expected data (storage systems, backup jobs, and so on) appears in VSC after you complete upgrade from a 32-bit system to VSC 5.0.

11. **(VSC 4.x system)** When your VSC 5.0 installation is running and you have verified that it has the correct data, uninstall the VSC 4.x program.

    You can use one of the following methods to uninstall VSC 4.x:

    - Go to the Windows Add or Remove Programs list and remove VSC 4.x.
    - Perform a "silent" uninstall by entering the following at the command line:

      `installer.exe /s /v"/qn /Li logfileREMOVE=ALL INSTALLDIR= \"`*`install_path`*`\" "`

Uninstalling VSC for VMware vSphere using Add/Remove Programs

You can uninstall the VSC for VMware vSphere software from your system using the Windows Add or Remove Programs list.

About this task

The uninstall program removes the entire VSC for VMware vSphere application. You cannot specify which capabilities you want to uninstall.

Steps

1. On the Windows server where you installed the VSC for VMware vSphere software, select **Control Panel > Add/Remove Programs** (Windows Server 2003) or **Control Panel > Programs and Features** (Windows Server 2008).
2. Select Virtual Storage Console for VMware vSphere and click **Remove** to immediately remove the program or click **Change** to start the installation wizard.
3. If you select **Change**, then click **Yes** to confirm that you want to remove the program.
4. In the installation wizard, select the **Remove** option and click **Next**.
5. Click **Remove** to uninstall the VSC for VMware vSphere software.

   After the process completes, a confirmation prompt is displayed.

   Note: At the confirmation prompt, click **Yes** to remove all the metadata files from the installation directory or click **No** so that you can manually delete the files in the directory.

Uninstalling VSC for VMware vSphere using silent mode

You can uninstall Virtual Storage Console for VMware vSphere using silent mode instead of the Windows Add/Remove Program. When you use silent mode, you can enter a command line that lets you automatically uninstall all the VSC features at once.

Before you begin

You must be logged on with administrator privileges to the machine from which you are uninstalling VSC.

Step

1. Use the following command line to uninstall VSC: `installer.exe /s /v"/qn /Li logfileREMOVE=ALL INSTALLDIR=\"installation path\""`

   This command removes all the VSC features.

Example

The following is an example of the command line you might use if you were uninstalling VSC 5.0 from a 64-bit host machine:

```
VSC-5.0-win64.exe /s /v"/qn /Li uninstall.log REMOVE=ALL
```

VASA Provider for clustered Data ONTAP installation

Virtual Storage Console for VMware vSphere is the management console for VASA Provider. Because of this dependency, the VASA Provider installation software is available for download from the Virtual Storage Console 5.0 for VMware vSphere Download page as well as from the VASA Provider for Clustered Data ONTAP Download page. These pages are located on the NetApp Support Site at *support.netapp.com*.

After you install VASA Provider, you must register it with VSC, then log out of the VMware vSphere Web Client. When you log back into the VMware vSphere Web Client and go to the VSC page, VSC displays a link to the VASA Provider GUI, which enables you to create storage capability profiles, assign the profiles to existing storage, and set up thresholds for alarms.

If you need to adjust settings for VASA Provider or perform maintenance tasks, you can use the VASA Provider maintenance menus, which are accessible from the console of the virtual appliance. The Main Menu provides several options for configuring VASA Provider and performing diagnostic operations. In addition, you can use the Vendor Provider Control Panel screen located at http://vm_ip:9080 to generate a support bundle.

Note: If you need to create a support bundle, you should use the Vendor Provider Control Panel to generate it. The Vendor Provider Control Panel creates a more complete bundle than the maintenance menu creates.

VASA Provider supported configurations

VASA Provider for clustered Data ONTAP requires Virtual Storage Console for VMware vSphere and is supported on specific releases of ESX/ESXi, vSphere, and Data ONTAP software. See the Interoperability Matrix, which is online at *support.netapp.com/matrix*, for details.

Note: These requirements were true at the time VSC 5.0 was released; however, they are subject to change. You should check the Interoperability Matrix and the Release Notes to see if any changes have been made.

Disk requirements

Before you install VASA Provider, you must make sure you have sufficient disk space. The recommended disk space is:

- 2.1 GB for thin provisioned installations
- 54.0 GB for thick provisioned installations

vSphere server configuration

VASA Provider requires that you have vCenter Server 5.5.

Host configuration

The required host configuration includes the following:

- Hosts: ESX/ESXi 4.0 and higher
- Virtual Hardware Version: 7
- Recommended memory: 8 GB RAM
- Recommended CPUs: 4

VASA Provider does not support the following:

- Having more than one VASA Provider registered with VSC at one time
- Direct-connect Storage Virtual Machines (SVMs, formerly known as Vservers)
- Qtree datastores
- VMFS datastores that span multiple LUNs
- FlexVols that are exposed by using multiple LIFs as multiple datastores
- SnapVault
- Load sharing
- IPv6

Installing VASA Provider for clustered Data ONTAP

You deploy the VASA Provider for clustered Data ONTAP virtual appliance on an ESXi host. After the VASA Provider virtual appliance is installed, you must register it with Virtual Storage Console for VMware vSphere.

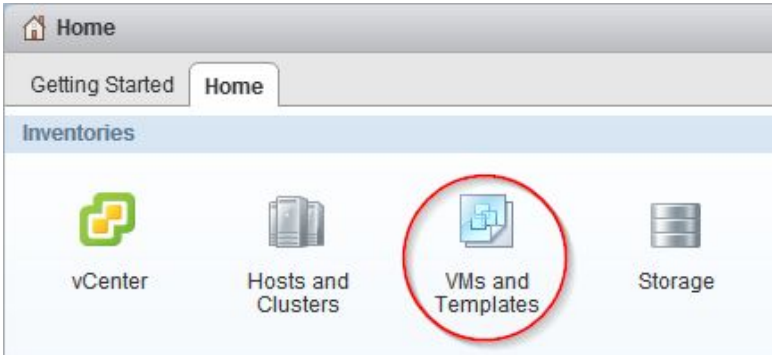
Before you begin

- (Recommended) You should download the VASA Provider software to your server before installing it.
- You must have a DNS entry for VASA Provider.

VASA Provider does not support direct-connect Storage Virtual Machines (SVMs, formerly known as Vservers) or qtree datastores.

Steps

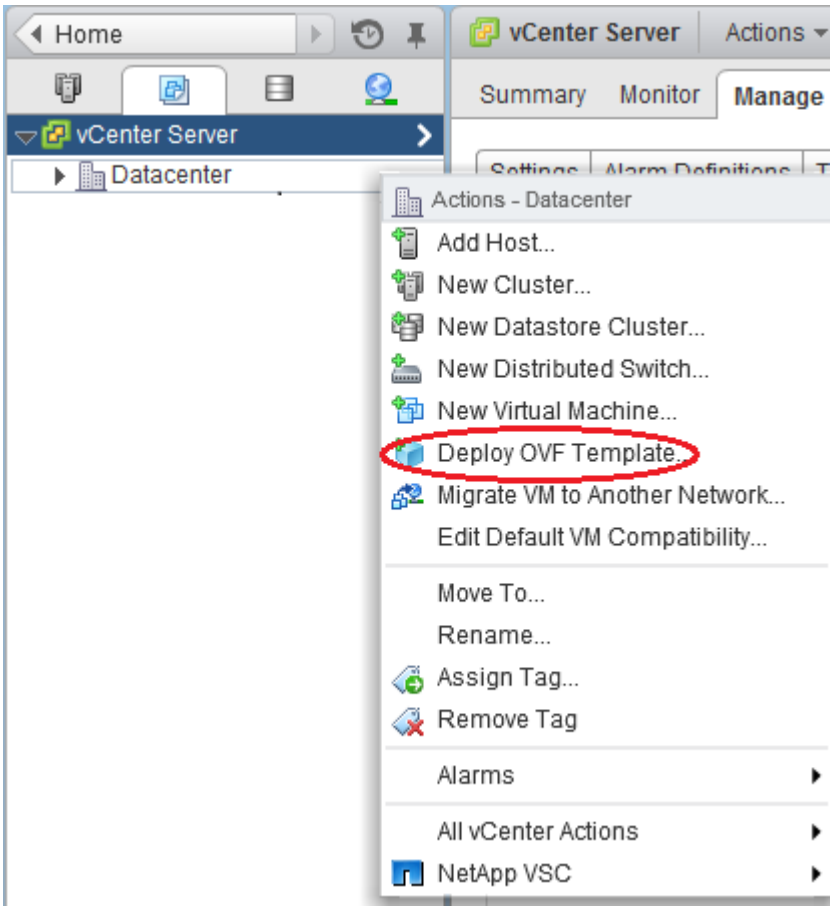
1. From the vSphere Web Client **Home** page, click **VMs and Templates**.



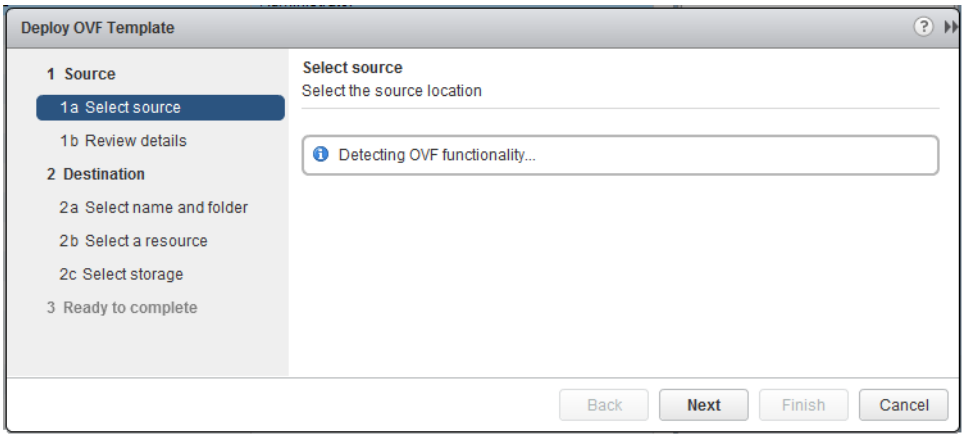
2. Right-click the datacenter where you want to deploy the VASA Provider software.

   The Actions pop-up menu appears.

3. Select the option **Deploy OVF template**.



This starts a wizard to step you through the process of installing the VASA Provider software. Follow the instructions provided on each page of the wizard.



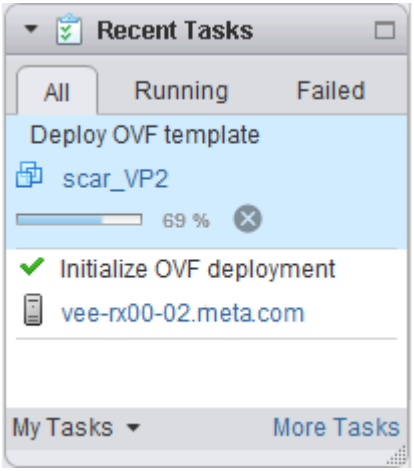
Some points to keep in mind include the following:

Page/Field	Explanation
Select source	Specify either the URL to the VASA Provider software or browse to location where you downloaded the software. You can install VASA Provider from a URL; however, the installation is usually faster if you download the software to your local machine. **Note:** If you download the software and the download process changes the file extension from .ova to .tar, you must rename the file to change the extension back to .ova.

Accept EULAs	Click **Accept** here even though there is no EULA. This screen provides information about the steps you must perform to complete the installation after you set up the VASA Provider virtual appliance. These steps include: • Powering on the virtual applliance by clicking the **Console** tab in the vCenter client. **Note:** You can check the option in the wizard to do this automatically. • Watching the console output for final instructions and your virtual appliance URL.
Select name and folder	Provide both a name that allows you to easily identify the virtual appliance and a location for the virtual appliance. The location can be either a folder or a datacenter.
Select a resource	Specify where you will deploy VASA Provider. This can be either a cluster, host, vApp, or resource pool.
Select storage	Specify both the virtual disk format and the location where you want to store files for the deployed template from the list of available datastores. The wizard displays a list of datastores that destination resource you selected in the previous page can access.
Setup networks	From the available networks shown, select the ones that you want to use with the deployed template. **Note:** IPv6 is not supported.

Customize template	If you are using DHCP, leave these fields blank. Otherwise, you can specify properties to customize the deployment information for VASA Provider. If you choose to provide custom settings, you must supply values for all the fields on this page. You cannot supply information for some fields and leave the rest blank. In addition, you must have created a DNS entry for VASA Provider before you enter information on this page.
Ready to complete	(Recommended) Select Power on after deployment. To complete your installation, you will need to power on the new virtual appliance and launch the console to supply passwords for both the maintenance account (maint) and VASA Provider account (vpserver). Review your settings. If you need to change something, go back to that page in the wizard.

4. Monitor the status of the Deploy OVF Template operation in the **Recent Tasks** pane.



When the operation completes, verify the application status. The status will continue to say that it is "initializing the DB" until you log in and log out. The status changes to "vpserver is running and waiting for vSphere registration."

Note: The current application status on the login screen only refreshes when the login process updates the page.

The new VASA Provider virtual appliance boots, requests that you install VMware tools, reboots, launches the console, and displays a pop-up window that starts you in Standard mode. You can use maintenance mode to modify information about the appliance from the command line GUI.

Note: When you are working within the console, your mouse disappears. To get it back, press Ctrl-Alt.

If the new VASA Provider does not power on automatically, click its name in the Recent Tasks pane. When it opens, you can use the Actions menu to power it on and then launch the console.

5. At the prompts, enter a password for the maintenance account (maint) and the vpserver account.

   (Recommended) Use different passwords for these two accounts. You will use the vpserver account password to register VASA Provider with VSC.

   Note: The application status is updated every 60 seconds; however, the display does not update unless you press Enter.

After you finish

After you install VASA Provider, you must register it with VSC. You do this from with the VSC Configuration page. You will need to supply the IP address for VASA Provider and the vpserver password.

Related tasks

Registering VASA Provider for clustered Data ONTAP with VSC for VMware vSphere on page 64

Maintaining VASA Provider for clustered Data ONTAP

You can perform maintenance tasks associated with the VASA Provider for clustered Data ONTAP from the command line interface. The menus that appear allow you to perform numerous tasks, including manage network and server issues, set up SSH, generate the vpserver support bundle, and run diagnostics.

Steps

1. If the VASA Provider is not currently powered on, go to its Summary page and select the power on option.
2. Launch the console.

   Note: When you are working within the console, your mouse disappears. To get it back, press Ctrl-Alt.

3. Log in to the maintenance account (maint).
4. In the Main Menu, select the menu for the task that you want to perform.

Note: From the submenus, you can use the "b" for back and "x" for exit keys as you navigate through them.

From the Main Menu, you can choose menus that allow you to perform the following tasks:

- Upgrade the VASA Provider
- Configure networks
- Configure your system
- Configure applications
- Perform support and diagnostic operations
- Generate of support bundles

Deleting VASA Provider for clustered Data ONTAP

You can delete the VASA Provider for clustered Data ONTAP from the vCenter Server if you no longer need it.

About this task

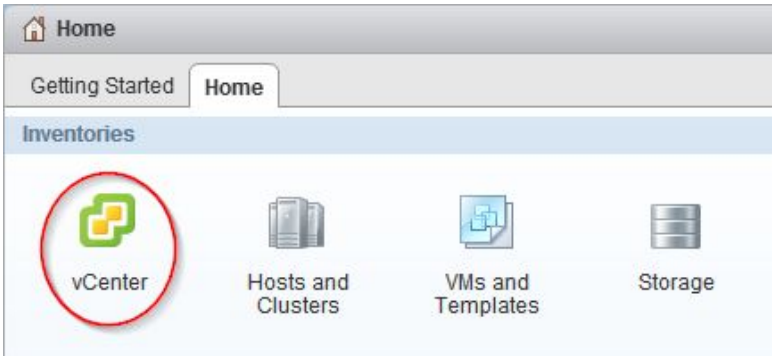
The vCenter Server gives you the choice of either deleting the VASA Provider from the disk or removing it from the inventory. If you do not plan to use the VASA Provider, you should choose the Delete from Disk option and remove it completely from the disk. If you choose the Remove from Inventory option, the VASA Provider is removed from the VMware inventory, but it remains on the disk.

Steps

1. Unregister VASA Provider from Virtual Storage Console for VMware vSphere.

   From the vSphere Web Client's Home page, click **Virtual Storage Console > Configuration > Register/Unregister VASA Vendor Provider**. Enter the vpserver password and select **Unregister.**

2. Locate the VASA Provider virtual appliance in the vCenter GUI. From the vSphere Web Client **Home** page, click **vCenter**.



3. Select the VASA Provider and power it off.
4. From the Actions menu, select **All vCenter Actions > Delete from Disk**.

NetApp NFS Plug-in for VAAI installation

The NetApp NFS Plug-in for VMware VAAI is not shipped with Virtual Storage Console for VMware vSphere; however, you can get the plug-in installation package and instructions for installing it from the NetApp Support Site at *support.netapp.com*. You can then go to use the Virtual Storage Console **Tools > NFS VAAI** page to complete your installation.

The plug-in is a software library that integrates the VMware Virtual Disk Libraries that are installed on the ESXi host. It is a good practice to install the plug-in because VAAI (VMware vStorage APIs for Array Integration) features such as copy offload and space reservations can improve the performance of cloning operations.

The plug-in is supported on systems running ESXi 5.0 or later with vSphere 5.0 or later and clustered Data ONTAP 8.1 or later or Data ONTAP 8.1.1 or later operating in 7-Mode.

To download the plug-in, go to the Software Download page on the NetApp Support Site and log in. In the row "NetApp NFS Plug-in for VAAI," select ESXi and click **Go!**. Continue through the pages until you reach NetApp NFS Plug-in for VMware VAAI Download. This page provides links to both the installation package and the installation guide.

Follow the VSC installation instructions in *Installing the NetApp NFS 1.0.20 Plug-in for VMware VAAI*.

After you install the plug-in, you must reboot the host. VSC then automatically detects the plug-in and uses it. You do not need to perform additional tasks to enable it.

Configuring your VSC for VMware vSphere environment

Virtual Storage Console for VMware vSphere supports numerous environments. Some of the features in these environments might require additional configuration. In some cases, you might need to perform maintenance operations.

Some of the configuration and maintenance work that you might need to perform includes the following:

- Verify your ESX host settings, including UNMAP
- Add timeout values for guest operating systems.
- Manually register VSC.
- Regenerate a VSC SSL certificate.
- Verify that you have the correct port settings.
- Set up connection brokers to work with the provisioning and cloning operations.
- Register VASA Provider and create storage capability profiles and threshold alarms.
- Work with the preferences file to enable datastore mounting across different subnets.

ESX server and guest operating system setup

Most of your ESX server values should be set by default; however, it is a good practice to verify the values and make sure the are right for your system setup. Virtual Storage Console for VMware vSphere also provides ISO files to enable you to set the correct timeout values for guest operating systems.

Configuring ESX server multipathing and timeout settings

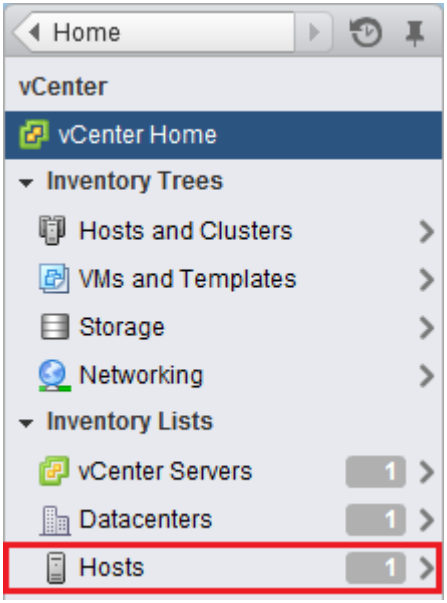
Virtual Storage Console for VMware vSphere checks and sets the ESX or ESXi host multipathing and HBA timeout settings that ensure proper behavior with NetApp storage systems.

Before you begin

This process might take a long time, depending on your configuration and system load. The task progress is displayed in the **Recent Tasks** panel. As tasks complete, the host status Alert icons are replaced by Normal or Pending Reboot icons.

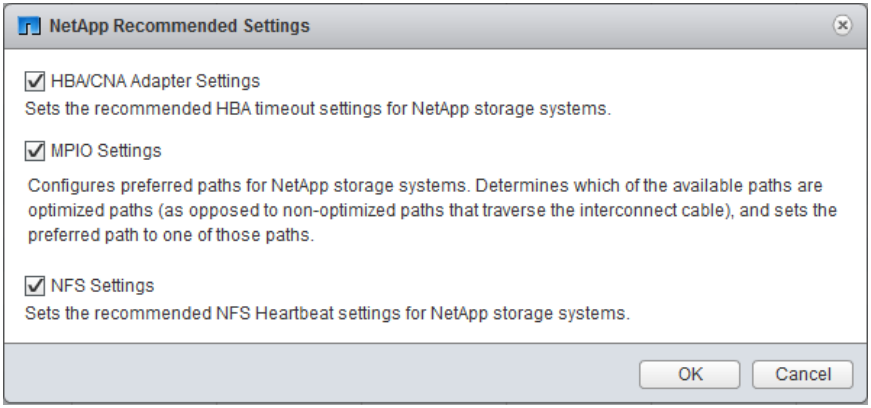
Steps

1. From the VMware vSphere Web Client **Home** page, click **vCenter > Hosts**.



2. Right-click on a host and select **Actions > NetApp VSC > Set Recommended Values** .
3. In the Recommended Settings pop-up box, select the values that work best with your system.

   The standard, recommended values are set by default.



4. Click **OK**.

ESX host values set by VSC for VMware vSphere

Virtual Storage Console for VMware vSphere sets ESX or ESXi host timeouts and other values to ensure best performance and successful failover. The values that VSC sets are based on internal NetApp testing.

VSC sets the following values on an ESX or ESXi host:

ESX advanced configuration

/VMFS/hardwareacceleratedlocking	Set to 1.

NFS settings

Net.TcpipHeapSize	If you are using vSphere 5.0 or later, set to `32`. For all other NFS configurations, set to `30`.
Net.TcpipHeapMax	If you are using vSphere 5.0 or later, set to `128`. For all other NFS configurations, set to `120`.
NFS.MaxVolumes	If you are using vSphere 5.0 or later, set to `256`. For all other NFS configurations, set to `64`.
NFS.HeartbeatMaxFailures	Set to `10` for all NFS configurations.
NFS.HeartbeatFrequency	Set to `12` for all NFS configurations.
NFS.HeartbeatTimeout	Set to `5` for all NFS configurations.

FC/FCoE settings

Path selection policy	Set to `RR` (round robin) for ESX 4.0 or 4.1 and ESXi 5.x, FC paths with ALUA enabled. Set to `FIXED` for all other configurations. Setting this value to `RR` helps provide load balancing across all active/optimized paths. The value `FIXED` is for older, non-ALUA configurations and helps prevent proxy I/O. In other words, it helps keep I/O from going to the other node of a high availability pair (HA) in an environment that has Data ONTAP operating in 7-mode.
Disk.QFullSampleSize	Set to `32` for all configurations. This setting is available with ESXi 5.x and ESX 4.x. Setting this value helps prevent I/O errors. **Note:** vSphere 5.1 handles Task Set Full (QFull) conditions differently from vSphere 4.x and 5.0. For more information on QFull settings in vSphere 5.1, see knowledgebase article 1013944, which is online at *kb.netapp.com/support/index?page=content&id=1013944*.
Disk.QFullThreshold	Set to `8` for all configurations. This setting is available with ESXi 5.0 and ESX 4.x. Setting this value helps prevent I/O errors. **Note:** vSphere 5.1 handles Task Set Full (QFull) conditions differently from vSphere 4.x and 5.0. For more information on QFull settings in vSphere 5.1, see knowledgebase article 1013944, which is online at *kb.netapp.com/support/index?page=content&id=1013944*.

Emulex FC HBA timeouts	For ESX 4.0 or 4.1 or ESXi 5.x, use the default value.
QLogic FC HBA timeouts	For ESX 4.0 or 4.1 or ESXi 5.x, use the default value.

iSCSI settings

Path selection policy	Set to `RR` (round robin) for all iSCSI paths. Setting this value to `RR` helps provide load balancing across all active/optimized paths.
Disk.QFullSampleSize	Set to `32` for all configurations. This setting is available with ESX 4.x and ESXi 5.x. Setting this value helps prevent I/O errors. **Note:** vSphere 5.1 handles Task Set Full (QFull) conditions differently from vSphere 4.x and 5.0. For more information on QFull settings in vSphere 5.1, see knowledgebase article 1013944, which is online at *kb.netapp.com/support/index?page=content&id=1013944*.
Disk.QFullThreshold	Set to `8` for all configurations. This setting is available with ESX 4.x and ESXi 5.x. Setting this value helps prevent I/O errors. **Note:** vSphere 5.1 handles Task Set Full (QFull) conditions differently from vSphere 4.x and 5.0. For more information on QFull settings in vSphere 5.1, see knowledgebase article 1013944, which is online at *kb.netapp.com/support/index?page=content&id=1013944*.
QLogic iSCSI HBA IP_ARP_Redirect	Set to `ON` for all configurations.
QLogic iSCSI HBA timeouts	ql4xportdownretrycount (qla4022 driver), ka_timeout (qla4xxx driver), and KeepAliveTO timeout settings are set to `14` for iSCSI SAN booted ESX hosts, and set to 60 for non-SAN-boot configurations.

UNMAP setting turned off in ESX 5.x

On hosts running ESX 5.0, Virtual Storage Console for VMware vSphere automatically turns off the UNMAP (`VMFS3.EnableBlockDelete`) parameter by setting it to 0.

On ESX 5.1 hosts, 0 is the default value. If you change this value to 1 on either ESX 5.0 or 5.1,VSC automatically resets it to 0. For this value to take effect, you must apply the HBA/CNA Adapter Settings on the host.

To avoid any potential performance impact due to UNMAP operations, VMware disabled this feature beginning in ESXi 5.0 Update 2. VSC ensures that this feature is disabled with all versions of ESXi 5.x.

Timeout values for guest operating systems

The guest operating system (GOS) timeout scripts set the SCSI I/O timeout values for supported Linux, Solaris, and Windows guest operating systems. The timeout values help improve disk I/O behavior in a failover situation.

These scripts are provided as .ISO files. You can get a copy of the scripts by clicking **Tools > Guest OS Tools** from the Virtual Storage Console Home page. There are two scripts for each operating system:

- A 60-second script
- A 190-second script

In most cases, the recommended value is 60 seconds. Knowledge base article 3013622, which is online at *kb.netapp.com/support/index?page=content&id=3013622*, contains information you can use when deciding which timeout value to use.

You can mount and run the script from the vSphere client. The Tools panel provides URLs for the scripts.

To get the script containing the timeout values you want for your operating system, you must copy the correct URL from the Guest OS Tools page and mount it as a virtual CD-ROM in the virtual machine using the vSphere client. Make sure you install the script from a copy of Virtual Storage Console for VMware vSphere that is registered to the vCenter Server that manages the virtual machine. After the script has been installed, you can run it from the console of the virtual machine.

Adding the CD-ROM to a virtual machine

To enable installing the guest operating system scripts, you need to add the CD-ROM to a virtual machine if it does not exist.

Steps

1. In the vSphere Client, select the desired virtual machine and power it off.
2. Right-click the virtual machine and select **Manage > VM Hardware**.
3. Select **CD/DVD Drive** in the **New device** drop-down box and click **Add**.
4. Select **CD/DVD Drive** and then click **Next**.
5. Click **Use physical drive**.
6. Click **Next** several times to accept the default values.
7. Click **OK** to finish adding the CD-ROM.
8. Power on the virtual machine.

Installing guest operating system scripts

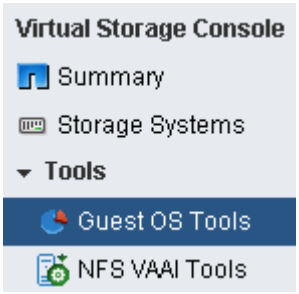
The ISO images of the guest operating system (GOS) scripts are loaded on the Virtual Storage Console for VMware vSphere server. Mount and run them from the vSphere Client to set the storage timeouts for virtual machines.

Before you begin

- The virtual machine must be running.
- The CD-ROM must already exist in the virtual machine or it must have been added.
- The script must be installed from the copy of the VSC registered to the vCenter Server that manages the virtual machine.

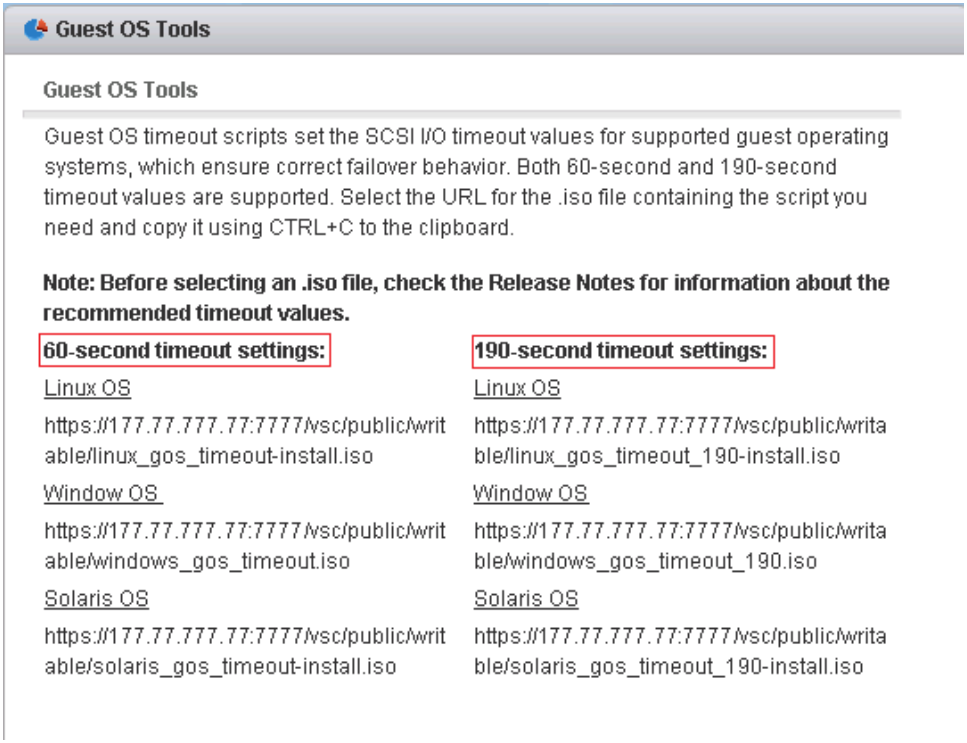
Steps

1. From the Virtual Storage Console **Home** page, expand **Tools** and click **Guest OS Tools**.



2. Under **Guest OS Tools**, use CTRL-C to copy the link to the ISO image for your guest operating system version to the clipboard.

   VSC provides both 60-second timeout scripts and 190-second timeout scripts for Linux, Windows, and Solaris. Select the script for your operating system that provides the timeout value you want to use.



3. Return to the VMware vSphere Web Client **Home** page and select **vCenter**.
4. Select the desired virtual machine and click the **Manage > VM Hardware**.
5. Select **CD/DVD Drive 1 > Connect to ISO image on local disk**.
6. Paste the link you copied into the **File Name** field and then click **Open**.

   Be sure that the link you are using is from the copy of the VSC running on the vCenter Server that manages the virtual machine.

After you finish

Log on to the virtual machine and run the script to set the storage timeout values.

Running the GOS timeout scripts for Linux

The guest operating system timeout scripts set the SCSI I/O timeout settings for RHEL4, RHEL5, RHEL6, SLES9, SLES10, and SLES11. You can specify either a 60-second timeout or a 190-second timeout. You should always run the script each time you upgrade to a new version of Linux.

Before you begin

You must mount the ISO image containing the Linux script before you can run it in the virtual machine.

Steps

1. Open the console of the Linux virtual machine and log in to an account with root privileges.
2. Run the `linux_gos_timeout-install.sh` script.

Result

For RHEL4 or SLES9, a message similar to the following is displayed:

```
Restarting udev... this may take a few seconds.
Setting I/O Timeout (60s) for /dev/sda - SUCCESS!
```

For RHEL5 or RHEL6, a message similar to the following is displayed:

```
patching file /etc/udev/rules.d/50-udev.rules
Hunk #1 succeeded at 333 (offset 13 lines).
Restarting udev... this may take a few seconds.
Starting udev: [ OK ]
Setting I/O Timeout (60s) for /dev/sda - SUCCESS!
```

For SLES10 or SLES11, a message similar to the following is displayed:

```
patching file /etc/udev/rules.d/50-udev-default.rules
Hunk #1 succeeded at 114 (offset 1 line).
Restarting udev ...this may take a few seconds.
Updating all available device nodes in /dev:         done
```

After you finish

Unmount the ISO image by clicking the **CD/DVD Connections** icon in the vSphere Client and selecting **CD/DVD Drive 1 > Disconnect from *`filename`*.iso**.

Running the GOS timeout scripts for Solaris

The timeout scripts set the SCSI I/O timeout settings for Solaris 10. You can specify either a 60-second timeout or a 190-second timeout.

Before you begin

You must mount the ISO image containing the Solaris script before you can run it in the virtual machine.

Steps

1. Open the console of the Solaris virtual machine and log in to an account with root privileges.
2. Run the `solaris_gos_timeout-install.sh` script.

Result

For Solaris 10, a message similar to the following is displayed:

```
Setting I/O Timeout for /dev/s–a - SUCCESS!
```

After you finish

Unmount the ISO image by clicking the **CD/DVD Connections** icon in the vSphere Client and selecting **CD/DVD Drive 1 > Disconnect from *filename*.iso**.

Running the GOS timeout script for Windows

The timeout scripts set the SCSI I/O timeout settings for Windows guest operating systems. You can specify either a 60-second timeout or a 190-second timeout. You must reboot the Windows guest OS for the settings to take effect.

Before you begin

You must mount the ISO image containing the Windows script before you can run it in the virtual machine.

Steps

1. Open the console of the Windows virtual machine and log in to an account with Administrator privileges.
2. If the script does not automatically start, open the CD drive and run `windows_gos_timeout.reg`.

   The Registry Editor dialog is displayed.
3. Click **Yes** to continue.

   The following message is displayed: `The keys and values contained in D:\windows_gos_timeout.reg have been successfully added to the registry.`
4. Reboot the Windows guest OS.

After you finish

Unmount the ISO image by clicking the **CD/DVD Connections** icon in the vSphere Client and selecting **CD/DVD Drive 1 > Disconnect from *filename*.iso**.

VSC for VMware vSphere configuration

Most of the Virtual Storage Console for VMware vSphere configuration happens automatically when you install the software. In some cases, you might need to register VSC with the vCenter Server or regenrate an SSL certificate.

It can also be helpful to know which VSC ports are available through the firewall.

Registering VSC for VMware vSphere with vCenter Server

After installing the Virtual Storage Console for VMware vSphere software, you must register it with vCenter Server. By default, the registration web page opens when the VSC for VMware vSphere installation is complete.

Before you begin

You must be logged on as a user with administrator privileges to the machine on which you install VSC. If you attempt to register VSC without having administrator privileges, the task does not complete correctly.

About this task

IPv6 addresses are not currently supported.

Steps

1. If the registration web page does not open automatically, type the following URL in a web browser:

   `https://localhost:8143/Register.html`

   `localhost` must be the computer where you installed VSC. If you are not performing this step from the computer where you installed VSC, you must replace `localhost` with the hostname or IP address of that computer.
2. If a security certificate warning appears, choose the option to ignore it or to continue to the web site.
3. In the Plugin service information section, select the IP address that the vCenter Server uses to access VSC.

   This IP address must be accessible from the vCenter Server. If you installed VSC on the vCenter Server computer, this might be the same address as the one you use to access the vCenter Server.
4. Type the host name or IP address of the vCenter Server and the administrative credentials for the vCenter Server.
5. Click **Register** to complete the registration.

   If you did not enter the correct user credentials for the vCenter Server, a registration failed error message appears. If that happens, you must repeat the previous steps.
6. Close the registration page after you complete the registration process because the web page is not automatically refreshed.

Regenerating an SSL certificate for VSC for VMware vSphere

The SSL certificate is generated when you install Virtual Storage Console for VMware vSphere. The distinguished name (DN) generated for the SSL certificate might not be a common name (CN)

("NetApp") that the client machines recognize. By changing the keystore and private key passwords, you can regenerate the certificate and create a site-specific certificate.

About this task

You might also need to regenerate the certificate if you are using the VSC backup and restore features. The certificate that is automatically generated for the SMVI process, which supports the backup and restore features, uses a weak algorithm. The certificate that you regenerate uses a stronger algorithm.

Steps

1. Stop the `vsc` service.

   There are several ways to do this. One way to stop the service is to use the Windows Services control panel.

2. Connect to the Windows console session or the Windows PowerShell console.

3. Go to the VSC installation directory and enter the following command:

   `bin\vsc ssl setup -cn <HOST>`

   For `<HOST>`, enter the host name of the system running VSC or a fully qualified domain name of the system running VSC.

   #### Example

   The following example executes the command from the installation directory and uses a host called `ESXiTester`:

   ```
   C:\Program Files\ NetApp\Virtual Storage Console>bin\vsc ssl setup -cn
   ESXiTester
   ```

4. At the prompt, enter the default keystore password:

   `changeit`

   You will also be prompted to enter a password for the private key (this can be any string you choose).

   Note: These commands work with Java JRE version 1.6.0_21. If you have a different version of Java installed in Program Files, your commands might be different.

   The following files are generated:

   - keystore file (default: `etc\nvpf.keystore`)
     This is the JKS keystore file.
   - keystore properties (default: `etc\keystore.properties`)
     This file contains the keystore file path and the keystore and key passwords. The administrator should secure this file and specify `http.ssl.keystore.properties` in `etc\nvpf.override` if the keystore properties file needs to be moved.

5. If you are using the VSC provisioning and cloning or optimization and migration features, perform the following two steps:
   a. Change to the VSC installation directory and enter the following command:

      `keytool -export -alias nvpf -keystore nvpf.keystore -file nvpf.cer`

      Example

      This example executes the command from the `etc` directory in the installation directory:

      ```
      C:\Program Files\NetApp\Virtual Storage Console\etc>keytool -export -
      alias nvpf -keystore nvpf.keystore -file nvpf.cer
      ```

      The command creates a new file called nvpf.cer.
   b. Import the certificate to the local a Java keystore by entering the command:

      `c:\Program Files\NetApp\Virtual Storage Console\etc>keytool -import -alias nvpf -file nvpf.cer -keystore "c:\Program Files\Java \jdk1.6.0_21\jre\lib\security\cacerts"`

6. If you are using the backup and restore features, perform the following steps to ensure that certificate is not using a weak algorithm:
   a. Copy the following entries from the keystore.properties file that you just created in the installation directory.

      The encrypted passwords might look similar but they are not an exact match to the following:

      ```
      http.ssl.key.password=1LKPQWaJIEvANxOqsF3ILKCKThDZv1F5
      ```

      ```
      http.ssl.keystore.file=C\:\\Program Files\\NetApp\\Virtual Storage
      Console\\etc\\nvpf.keystore
      ```

      ```
      http.ssl.keystore.password=u4SIS8KXhzMDq5JebwyF0AXT36YVCfvX
      ```
   b. If the `smvi.override` file exists, add these entries to the file, which is located at `http.ssl.keystore.file=C\:\\Program Files\\NetApp\\Virtual Storage Console\smvi\server\etc`

      If the `smvi.override` file does not exist, you must create it at that location and then add the entries.
   c. Restart the SMVI service
   d. Verify that the new certificate, generated with the sha1WithRSAEncryption algorithm, is being used.

      You can use a tool such as SSLScan to verify SSL certificates.

7. Secure the `etc\keystore.properties` file.

   There are several ways to do this, including the following:

   - If the installation directory is on a network share directory, move the file to local storage.
   - Move the file to storage accessible only to the SYSTEM user, which keeps unauthorized users from being able to view or modify the file.

8. Restart the `vsc` service.
9. You can review and accept the SSL certificate after the vSphere Client receives the certificate by clicking the NetApp icon in the vSphere Client.
10. Now import the SSL certificate into the Trusted Root Certification Authorities store to prevent SSL security warnings from appearing every time you launch the vSphere client.

    For details, see the documentation for your Windows operating system.

VSC for VMware vSphere port requirements

By default, Virtual Storage Console for VMware vSphere uses designated ports to enable communication between its components, which include storage systems and the VMware vCenter server. If you have firewalls enabled, you must ensure that the firewalls are set to allow exceptions.

For firewalls other than Windows, you must manually grant access to specific ports that VSC uses. If you do not grant access to these ports, an error message such as `Unable to communicate with the server` is displayed.

VSC uses the following default ports:

Default port number	Description
443	The VMware vCenter Server and the storage systems listen for secure communications using secure HTTP (SSL) on this port.
80	The VMware vCenter server and the storage systems listen for standard, unencrypted communication via standard HTTP on this port.
8143	VSC listens for secure communication on this port.
8043	The VSC backup and restore features and the VSC Restore Agent and CLI listen for secure communication on this port.

Managing connection brokers

You can use the Connection brokers panel to view and manage the connection brokers available for importing clone data at the end of the clone operation.

- For VMware View Server, clone data is imported into View Server at the end of the clone operation.
- For Citrix XenDesktop, a `.csv` file is created in the directory `c:\program files\netapp \virtual storage console\etc\kamino\exports`. See *Cloning virtual machines* on page 116 for details.

To work with connection brokers in Virtual Storage Console for VMware vSphere, you must have .Net 3.5 available on the system where you have VSC installed. For some versions of Windows, such as Windows 2008, .Net 3.5 is included as part of the installation. For other versions, such as Windows 2003, it is not part of the base install, so you must manually install it.

Adding connection brokers

You can add connection brokers to Virtual Storage Console for VMware vSphere.

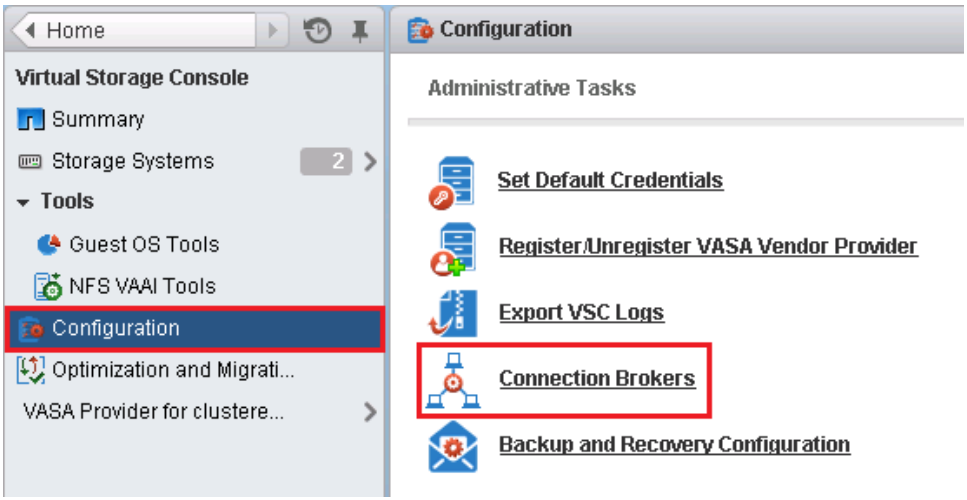
Before you begin

To work with connection brokers, you must have .Net 3.5 available on the system where you have VSC installed. For some versions of Windows, such as Windows 2008, .Net 3.5 is included as part of the installation. For other versions, such as Windows 2003, it is not part of the base install, so you must manually install it.

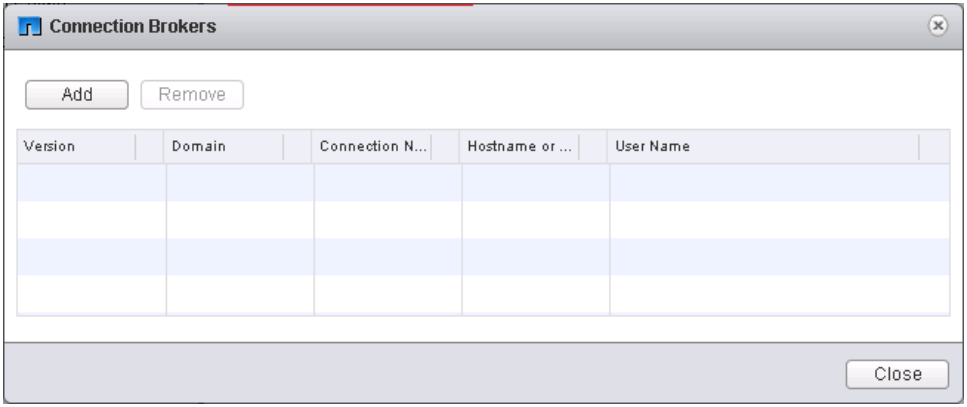
To ensure that your configuration is supported, check the Interoperability Matrix, which is available online at *support.netapp.com/matrix*.

Steps

1. From the Virtual Storage Console **Home** page, select **Configuration** > **Connection brokers**.



2. In the pop-up **Connection Brokers** box, click **Add**.



3. In the **Add Connection Broker** window, specify the following information:
   a. **Connection Broker Version** - Select the connection broker name and version from the drop-down list.
   b. **Domain** - Enter the domain containing the connection broker.
   c. **Connection name** (XenDesktop 5.0 only) - Enter the name given the Citrix XenDesktop 5.0 connection.
   d. **Hostname or IP Address** (VMware View Server only) - Enter the connection broker hostname or IP address.
   e. **Username** (VMware View Server only) - Enter the domain user name.
   f. **Password** (VMware View Server only) - Enter the domain password.

Removing connection brokers

You can remove a connection broker from the list of available connection brokers.

Steps

1. From the Virtual Storage Console **Home** page, select **Configuration** > **Connection brokers**.
2. In the pop-up **Connection Brokers** box, click **Remove**.
3. Click **Yes** to confirm.

VASA Provider for clustered Data ONTAP configuration

You must register the IP address of VASA Provider for clustered Data ONTAP with Virtual Storage Console for VMware vSphere. After you do that, you can use the VASA Provider features to create storage capability profiles and to set up thresholds for alarms.

VASA Provider lets you create alarms to notify you when the volume and aggregate thresholds are approaching full capacity. It automatically notifies you if a datastore is no longer in compliance with its storage capability profile.

Registering VASA Provider for clustered Data ONTAP with VSC for VMware vSphere

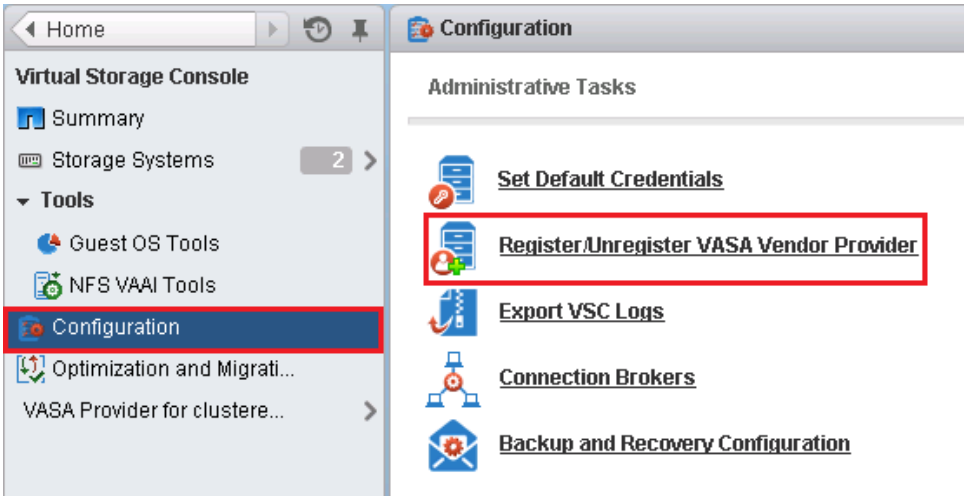
After you have installed VASA Provider for clustered Data ONTAP, you must register it with Virtual Storage Console for VMware vSphere.

Before you begin

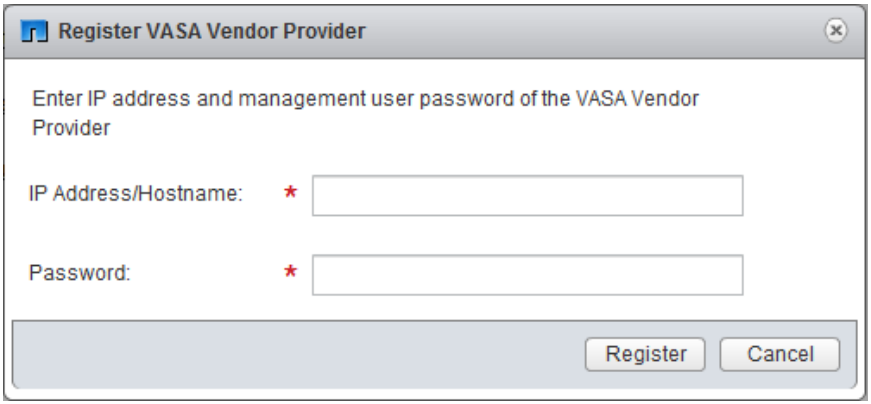
- You can only register one VASA Provider for a vCenter Server.
- You must have the IP address or FQDN for VASA Provider.
- You must have the password for the vpserver account for VASA Provider

Steps

1. From the Virtual Storage Console **Home** page, click **Configuration** > **Register/Unregister VASA Vendor Provider**.



2. In the Register VASA Vendor Provider pop-up box, enter the following information:
   - The IP address or hostname where you installed the VASA Provider
   - The password for the VASA Provider's vpserver account



3. Click **Register**.

   A pop-up box telling you the VASA Provider was successfully registered appears.

   You must log out of the vSphere Web Client and log back in again in order to see the VASA Provider interface. From this interface, you can set up storage capability profiles and assign them to datastores as well as set threshold alarms.

   Registering VASA Provider normally takes about 30 seconds. If you have an exceptionally large environment, it can take longer.

   Note: If you upgrade VSC, you must first unregister the VASA Provider.

Related tasks

Installing VASA Provider for clustered Data ONTAP on page 40

Creating and editing storage capability profiles

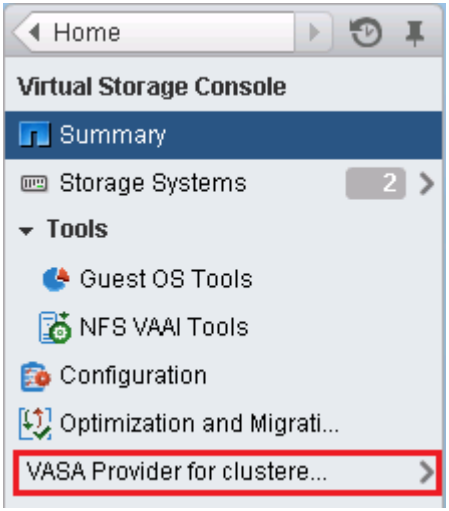
You have several options for using VASA Provider for clustered Data ONTAP to create new storage capability profiles. You can create a new profile manually, you can auto-generate a profile based on a datastore's capabilities, or you can clone an existing profile and modify it to meet your needs. After you have a profile set up, you can go back and edit it as needed.

Before you begin

You must have registered your VASA Provider with Virtual Storage Console for VMware vSphere before you perform these steps.

Steps

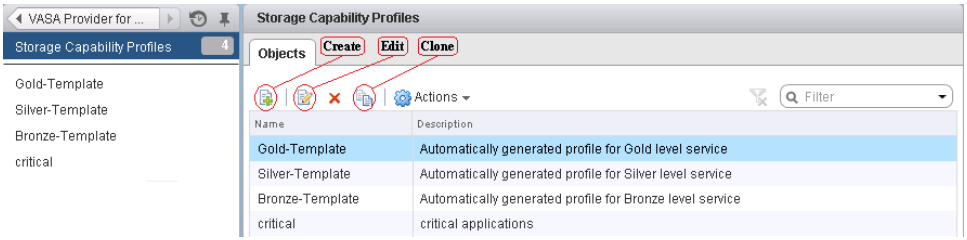
1. From the Virtual Storage Console **Home** page, click **VASA Provider for clustered Data ONTAP** to go to the VASA Provider GUI.



2. Select **Storage Capability Profiles**.

3. Choose the operation you want to perform:

To ...	Perform the following action ...
Create a new profile	Click the Create icon.
Edit an existing profile	Select the profile on the Objects page and choose either the Edit icon or Edit from the Actions menu.
Clone an existing profile	Select the profile on the Objects page and choose either the Clone icon or Clone from the Actions menu.



Note: To view the values associated with an existing profile, click the profile name in the Storage Capabilities Profile page. VASA Provider then displays the Summary page for that profile.

4. Complete the pages in the **Create storage capability profile** wizard to set up a profile or edit these values to modify an existing profile.

   Most of the fields in this wizard are self-explanatory. The majority of fields allow you to select a value from a drop-down list. As you run the wizard, here are some points to keep in mind:

Consideration	Explanation
Identifying multiple profiles	You can use the **Description** field on page 1 (Name and Description) to describe the purpose of the storage capability profile. Having a good description is useful because it is a good practice to set up different profiles based on the applications being used. For example, a business critical application requires a profile containing resources that support higher performance, good disaster recovery, and long retention. Enabling these features on datastores can be costly. If the datastores are only needed for basic applications, you might be able to reduce cost by creating a more moderate profile.

Consideration	Explanation
Any value will do for a field	If you don't require a specific value for a resource, you can select the **Any** value. VASA Provider then ignores that field when it searches for a matching profile. **Note:** VASA Provider does not support storage capability profiles that consist of only fields with the **Any** value. You can supply this value for multiple fields, but you must also specify one or more specific values for the profile. VASA Provider uses the values you supply when it creates a filter to locate available datastores. It displays these datastores when you view them in the Storage Mapping page or use storage capability profiles to provision storage. For example, if on page 6 of the wizard(Space Efficiency) you select **Yes** as the value for Autogrow, VASA Provider only matches the profile to a datastore if the volume has Autogrow enabled and it matches the other profile values. If you select **No**, then Autogrow must be disabled for that profile to be considered. However, if you select **Any** as the value, VASA Provider ignores that feature when it checks to see if the datastore matches the profile.
Quality of service functionality	Selecting either **IOPS** or **MBPS** as the measurement for the Throughput Limit field on page 4 (Performance) enables you to use quality of service functionality. Keep in mind that **IOPS** is a precise measurement. If you request 1400 **IOPS**, but the datastore is provisioned with 1300 **IOPS**, the datastore will not match that profile.

5. When you have the features you want selected, click OK.

After you finish

After you create a profile you can return to the **VASA Provider for clustered Data ONTAP** page and select **Storage Mapping** to see which profiles match which datastores.

Related tasks

Mapping storage to storage capability profiles on page 71
Auto-generating storage capability profiles on page 73
Provisioning datastores on page 113

Setting alarm thresholds in VASA Provider for clustered Data ONTAP

VASA Provider for clustered Data ONTAP enables you to set alarms for volume thresholds and aggregate thresholds. For both of these, you can specify a percent nearly full threshold and a percent full threshold. VASA Provider displays a yellow alarm when the nearly full limit is reached and a red alarm when the full limit is reached.

Before you begin

You must have registered your VASA Provider with Virtual Storage Console for VMware vSphere.

About this task

You cannot provision virtual machines onto a datastore that has a red alarm.

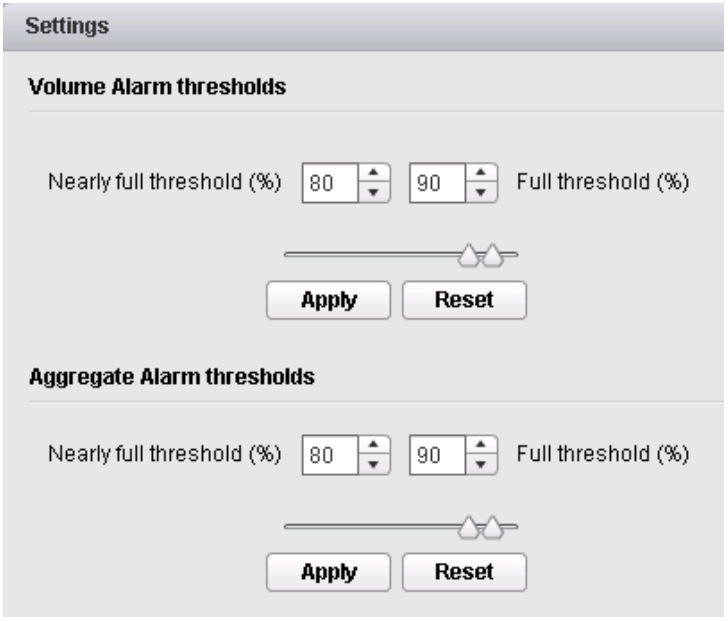
Threshold alarms take precedence over alarms about noncompliance between datastores and profiles. If there is a yellow or red threshold alarm, VASA Provider does not report any noncompliance issues for any associated datastores.

Steps

1. From the Virtual Storage Console **Home** page, click **VASA Provider for clustered Data ONTAP** to go to the VASA Provider GUI:

2. Select **Settings**:

3. Specify the percent values for “Nearly full threshold (%)” and “Full threshold (%)” for both the volume and the aggregate:



When setting the values, keep the following information in mind:

- Clicking **Reset** returns the values to the previous values.
  It does not return them to the default values of 80% for nearly full and 90% for full.
- There are two ways to set the values:
  - Use the up and down arrows next to the values to adjust them.
  - Slide the arrows on the bar below the values to adjust them.
- The lowest value you can set for the “Full threshold (%)” values for volumes and aggregates is 6%.

4. When you have the values you want, click **Apply**.

   You must click **Apply** for both the volume alarm and the aggregate alarm.

5. Perform these steps for both the volume alarm thresholds and the aggregate alarm thresholds.

Mapping storage to storage capability profiles

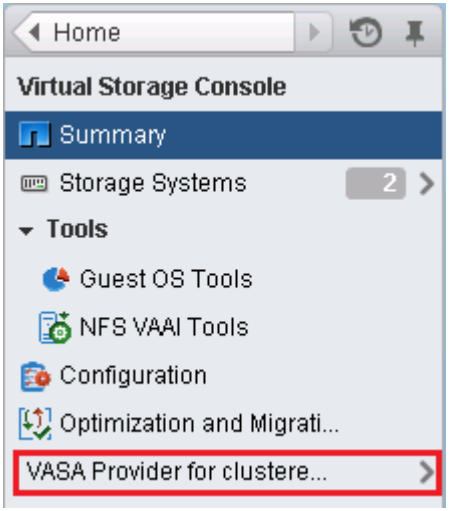
You can map the datastores associated with the VASA Provider for clustered Data ONTAP to storage capability profiles. You can assign a profile to a datastore that does not have one or change the current profile associated with a datastore.

Before you begin

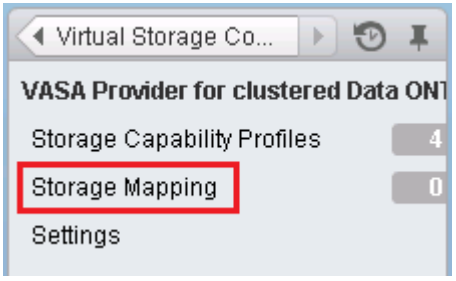
- You must have registered your VASA Provider with Virtual Storage Console for VMware vSphere before you perform these steps.
- VSC must have already discovered your storage.

Steps

1. From the Virtual Storage Console **Home** page, click **VASA Provider for clustered Data ONTAP** to go to the VASA Provider GUI.



2. Select **Storage Mapping**.



From this page, you can determine the following information:

- How many profiles match the datastore.

  Note: The Storage Mapping page does not display any qtree datastores. VASA Provider does not support qtree datastores.

- Whether the datastore is currently associated with a profile.

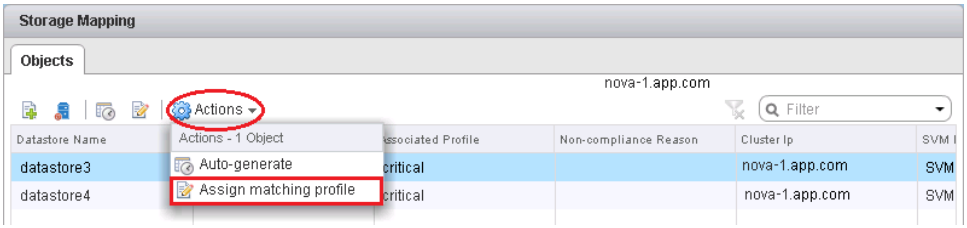
  Note: A datastore can match multiple profiles, but it can only be associated with one profile.

- Whether the datastore is complaint with the profile associated with it.

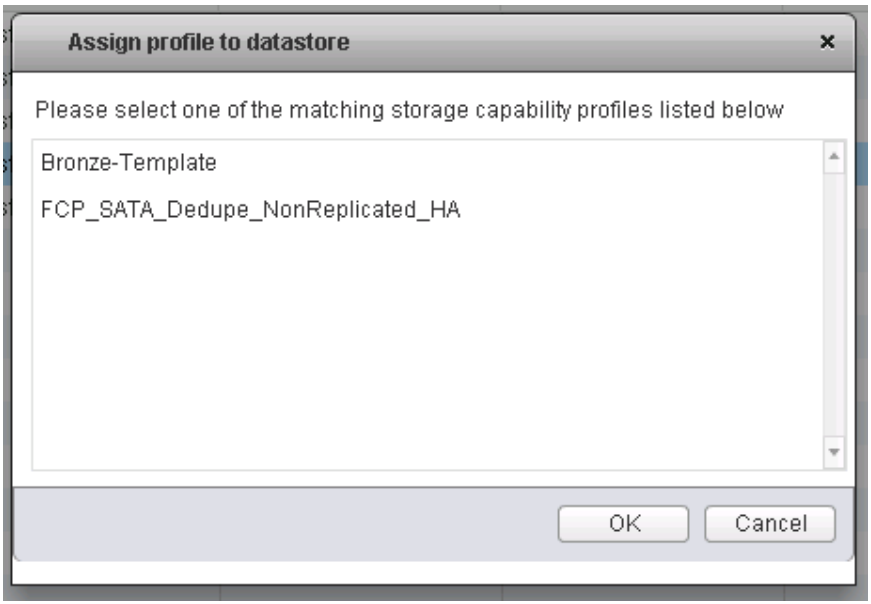
3. To map a profile to a datastore or change a datasore's existing profile, select the datastore.

   Note: To locate specific datastores or other information on this page, you can use the Search box to enter a name or a partial string. VSC displays the search results separately. To return to the full display, remove the text from the Search box and press Enter.

4. From the Actions menu, select **Assign matching profile**.



5. Select the profile you want map to the datastore from the list of matching profiles provided in the **Assign datastore to profile** pop-up.



You must refresh the screen to see the new assignment.

Auto-generating storage capability profiles

VASA Provider for clustered Data ONTAP enables you to auto-generate storage capability profiles from existing datastores. When you select a datastore from the Storage Mapping page and click **Auto-generate**, VASA Provider reverse engineers that datastore to create a profile that contains capabilities used by that datastore.

Before you begin

- You must have registered your VASA Provider with Virtual Storage Console for VMware vSphere before you perform these steps.
- VSC must have already discovered your storage.

About this task

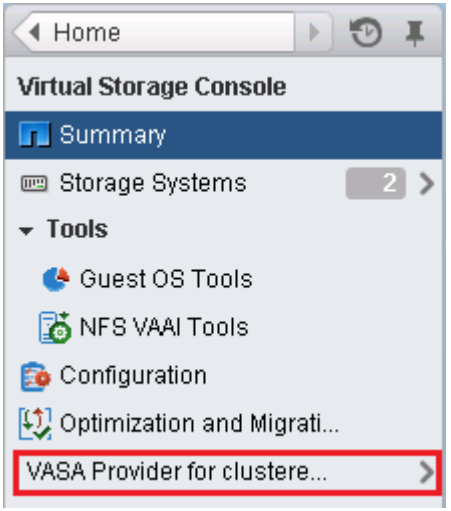
Profiles created by reverse engineering contain only information about the following capabilities:

- High availability
- Protocol
- Disk Type
- Flash Pool
- Deduplication
- Replication

After you create the profile, you can modify it to include more capabilities. The Create storage capability profile wizard provides information on the capabilities you can include in a profile.

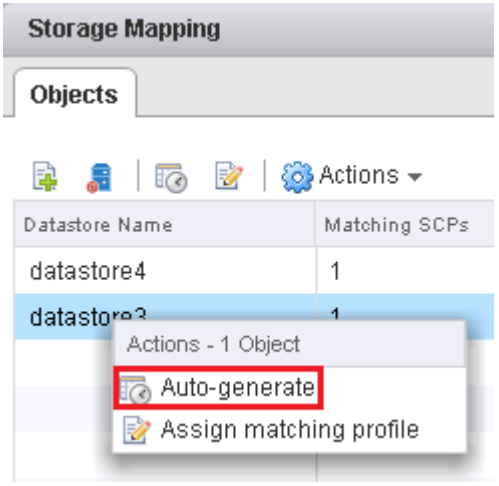
Steps

1. From the Virtual Storage Console **Home** page, click **VASA Provider for clustered Data ONTAP** to go to the VASA Provider GUI.



2. Select **Storage Mapping**.

3. From the list on the **Objects** page, select a datastore.
4. From the Actions menu, select **Auto-generate**.



5. When Auto-generate completes, refresh the screen to see information about the new profile.

   The VASA Provider places the new profile in the Associated profile column. The name of the new profile is based on the resources in the profile. For example, a profile named "FCP_SATA_NoDedupe_NonReplicated_HA" has the following configuration:

   - FCP protocol
   - SATA disk
   - No deduplication
   - No replication
   - High Availability enabled

   You can rename the profile, if you so choose.

Checking for datastore compliance with the mapped storage capability profile

You can quickly check to see whether your datastores are still compliant with the storage capability profiles mapped to them.

Before you begin

- You must have registered your VASA Provider with Virtual Storage Console for VMware vSphere before you perform these steps.
- VSC must have already discovered your storage.

Steps

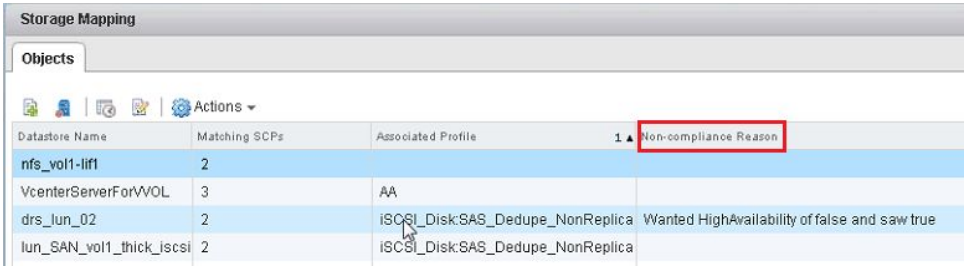
1. From the Virtual Storage Console **Home** page, click **VASA Provider for clustered Data ONTAP** to go to the VASA Provider GUI.

2. Select **Storage Mapping**.

3. Look at the column **Non-compliance Reason**.

   Note: You can also click the Compliance check icon; however, doing that tells VSC to perform a rediscovery operation for all the storage, which can take a long time.

   If a datastore is no longer compliant with its profile, this column lists the reason. For example, a profile might require Flash Pool, but that setting has been changed on the underlying storage so that Flash Pool is no longer used.



After you finish

When you discover a datastore that is not compliant with its profile, you can either modify the settings on the volume backing the datastore to make it compliant, or you can assign the datastore a new profile.

To modify the settings go to the VASA Provider Storage Capability Profile page.

Configuring AutoSupport for backup jobs

Information about specific errors that occur during backup and restore operations is automatically sent to the EMS log files. Enabling AutoSupport in Virtual Storage Console for VMware vSphere ensures that events such as a backup failure because of an error in taking a VMware snapshot or making a Snapshot copy are also sent to the EMS logs.

Steps

1. From the vSphere Web Client **Home** page, click **Virtual Storage Console**.
2. In the navigation pane, click **Configuration > Backup and Recovery Configuration**.

3. In the **Backup and Recovery Configuration** dialog box, click the **Enable AutoSupport** check box to enable AutoSupport.

Related tasks

Collecting the VSC for VMware vSphere log files on page 155

Configuring email alerts for backup jobs

You can configure the email alert notifications for the Virtual Storage Console server to send alert notifications when a backup job runs. The information you provide in the Backup and Recovery Configuration dialog box is then populated in the Schedule Backup wizard and you do not have to type this information for every backup job.

Before you begin

The following information must be available:

- Email address from which the alert notifications are sent
- Email address to which the alert notifications are sent
- Host name to configure the SMTP server

Steps

1. From the vSphere Web Client **Home** page, click **Virtual Storage Console**.
2. In the navigation pane, click **Configuration > Backup and Recovery Configuration**.
3. In the **Backup and Recovery Configuration** dialog box, specify the email address and SMTP server from which the alert notifications are sent as well as the email server to which the alert notifications are to be sent.
4. Optional: Click **Send Test Email** to verify that the outgoing email server to which the alert notifications are to be sent is working correctly.

The preferences files

The preferences files contain settings that control Virtual Storage Console for VMware vSphere operations. You should not need to modify the settings in these files, except in some rare situations.

There are two preferences files. The files include entry keys and values that determine how VSC performs operations. The files are stored in the following locations:

VSC_install_dir`\etc\kamino\kaminoprefs.xml`

VSC_install_dir`\etc\kamino\kaminosdkprefs.xml`

One reason to modify the preferences files is if you use iSCSI or NFS and the subnet is different between your ESX hosts and your storage system. In that situation, if you do not modify settings in the preferences files, provisioning a datastore will fail because VSC cannot mount the datastore.

Enabling datastore mounting across different subnets

If you use iSCSI or NFS and the subnet is different between your ESX hosts and your storage system, you need to modify two settings in the Virtual Storage Console for VMware vSphere preferences files. Otherwise, provisioning will fail because VSC cannot mount the datastore.

About this task

When datastore provisioning fails, VSC logs the following error:

```
Unable to continue. No ip addresses found when cross-referencing kernel ip addresses and addresses on the controller.
```

```
Unable to find a matching network to NFS mount volume to these hosts.
```

Steps

1. Open the following files in a text editor:

   VSC_install_dir`\etc\kamino\kaminoprefs.xml`

   VSC_install_dir`\etc\kamino\kaminosdkprefs.xml`

2. Update both files as follows:

If you use...	Do this...
iSCSI	Change the value of the entry key `default.allow.iscsi.mount.networks` from ALL to your ESX host subnet masks.
NFS	Change the value of the entry key `default.allow.nfs.mount.networks` from ALL to your ESX host subnet masks.

   The preferences files include example values for these entry keys.

   Note: ALL does not mean all networks. It means that all matching networks between the host and storage system can be used to mount datastores. Specifying subnet masks enables mounting across the specified subnets only.

3. Save and close the files.

Setting the frequency of NFS path optimization checks

By default, Virtual Storage Console for VMware vSphere checks the optimization of NFS paths every five minutes. You can change the frequency of these checks by modifying the `vscPreferences.xml` file.

Steps

1. In the `etc/vsc/vscPreferences.xml` file, add the following entry:

   `<entry key="default.server.path.optimization.sleep" value="`*`value_in_seconds`*`"/>`

   `value_in_seconds` is the amount of time, specified in seconds, that you want VSC to wait before rechecking the optimization of the NFS paths.

2. To confirm that the optimization checks are now occurring at the new interval, check the entries in the `log/vsc.log` log file.

   The log file contains statements, similar to the following, that enable you to determine how often the path checks are occurring:

```
2013-10-17 16:26:58,665 [Thread-16] DEBUG (PathOptimizationManager)
- Refreshing controllers and recalculating path optimization
details...
2013-10-17 16:26:58,667 [Thread-16] DEBUG (PathOptimizationManager) -
Path optimization detection complete.
```

Configuring vCenter Server Heartbeat to work with VSC for VMware vSphere

If you are using vCenter Server Heartbeat, you need to perform some additional steps to ensure it works with Virtual Storage Console for VMware vSphere.

Before you begin

VSC does not provide vCenter Server Heartbeat. That feature is available from VMware.

You must perform these steps when you have vCenter Server, vCenter Server Heartbeat, and VSC running locally on the same server.

Steps

1. Click **vCenter Server Heartbeat** > **Manage Server** and log into the Management GUI for the VMware vCenter Server Heartbeat Console.

2. Add either a secondary or primary server connection by clicking **Add Connection**.
3. Click **Applications** > **Services**.
4. Click **Add**.
5. Select the individual service listed, NetApp vSphere Plugin Framework (NVPF).
6. If you are using the VSC backup and restore features, select the "SMVI" service also.
7. Leave all service configurations to the default "recover service" and click OK.
8. Click **Data** > **File filters**.
9. Click **Add Inclusion Filter**.
10. Navigate to the VSC installation directory and select it.

    This directory is normally located at `<ProgramFiles>\NetApp\Virtual Storage Console`.

Result

All the files in Inclusion Filter are in sync between primary and secondary servers. The VSC service NVPF and, if you are using the backup and restore features, the SMVI service are being protected by vCenter Server Heartbeat.

For complete details about possible issues when using vCenter Server Heartbeat and VSC together, see VMware KB1036507: *Additional vCenter Server Heartbeat configurations for protecting a Virtual Storage Console.*

Authentication and user management with vCenter RBAC and Data ONTAP RBAC

Role-based access control (RBAC) is a process that enables administrators to control access to and user actions on vSphere objects and storage systems running Data ONTAP. Virtual Storage Console for VMware vSphere supports both vCenter Server RBAC and Data ONTAP RBAC.

The administrator handles setting up the RBAC roles. Depending on your system setup, you might have different administrators handling these two types of RBAC:

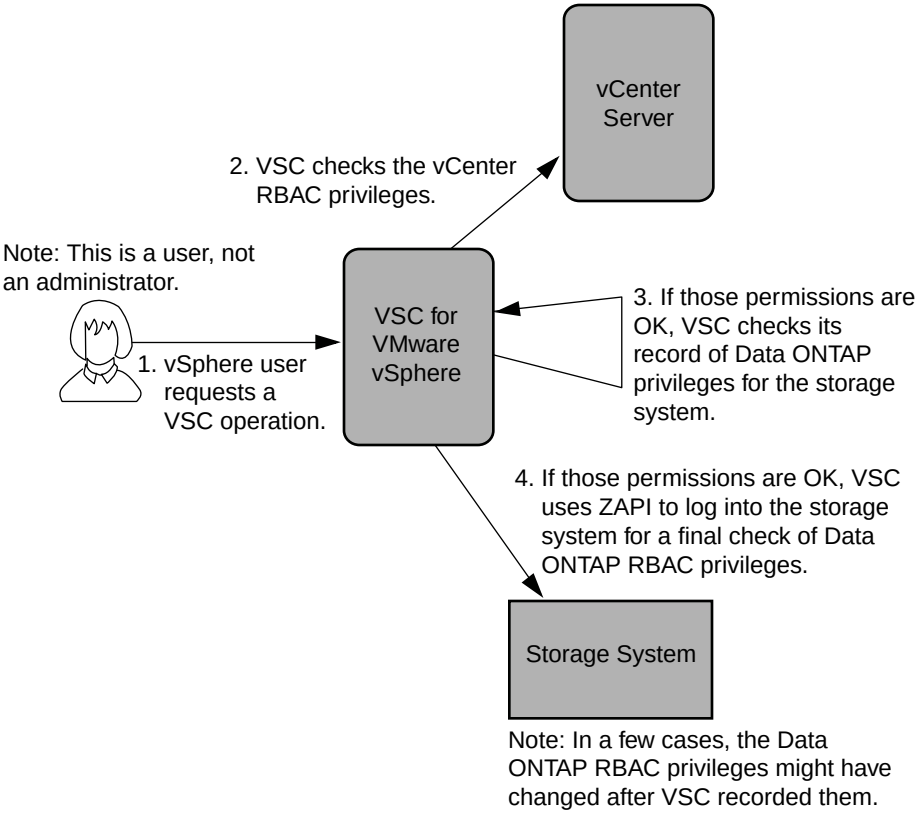
- **vCenter Server RBAC**
  This security mechanism restricts the ability of vSphere users to perform VSC tasks on vSphere objects, such as virtual machines, datastores, and datacenters.
  The vSphere administrator sets up vCenter Server RBAC by assigning permissions to specific vSphere objects, which are listed in the vSphere inventory. In many cases, a VSC task requires that more than one object have permissions. For this reason, it is a good practice to assign permissions on the root object (also referred to as the *root folder*). You can then restrict those entities that do not need permissions.

  Note: At a minimum, all users must have the VSC-specific, read-only View privilege assigned to them. Without this privilege, users cannot access the VSC GUI.

- **Data ONTAP RBAC**
  This security mechanism restricts the ability of VSC to perform specific storage operations, such as creating, destroying, or backing up storage for datastores, on a specific storage system.
  The storage administrator sets up Data ONTAP RBAC by defining storage credentials consisting of a user name and password in Data ONTAP. The storage credentials map to VSC storage operations. Then the administrator, usually the storage administrator, sets the storage credentials in VSC for each storage system that VSC manages. VSC uses a single set of credentials for each storage system.

VSC checks the vCenter Server RBAC permissions when a user clicks a vSphere object and initiates an action. If a user has the correct vCenter Server RBAC permission to perform that task on that vSphere object, VSC then checks the Data ONTAP credentials for the storage system. If those credentials are also confirmed, then VSC allows the user to perform that task.

The following diagram provides an overview of the VSC validation workflow for RBAC privileges (both vCenter and Data ONTAP):



Related concepts

vCenter Server role-based access control features in VSC for VMware vSphere on page 82
Standard roles packaged with VSC for VMware vSphere on page 87
Data ONTAP role-based access control features in VSC for VMware vSphere on page 91

vCenter Server role-based access control features in VSC for VMware vSphere

vCenter Server provides role-based access control (RBAC) that enables you to control access to vSphere objects. In Virtual Storage Console for VMware vSphere, vCenter Server RBAC works with Data ONTAP RBAC to determine which VSC tasks a specific user can perform on objects on a specific storage system.

To successfully complete a task, you must have the appropriate vCenter Server RBAC permissions. During a task, VSC checks a user's vCenter Server permissions before checking the user's Data ONTAP privileges.

You can set 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.

Components that make up vCenter Server permissions

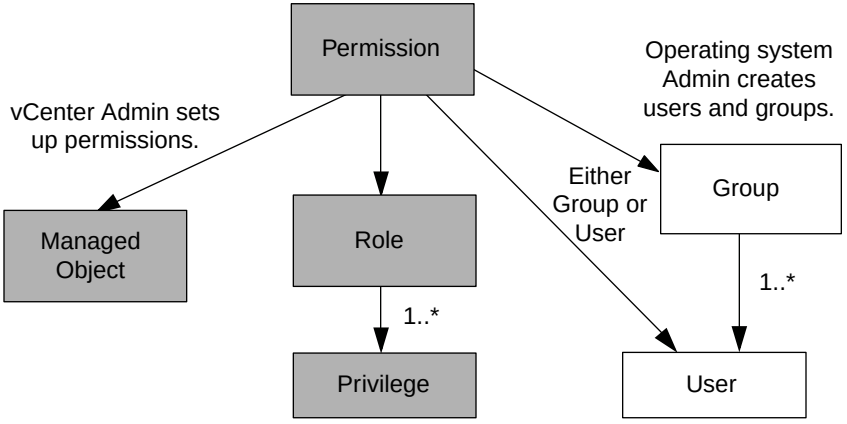
The vCenter Server recognizes permissions, not privileges. Each vCenter Server permission consists of three components.

These components are the following:

- One or more privileges (the role)
  The privileges define the tasks that a user can perform.
- A vSphere object
  The object is the target for the tasks.
- A user or group
  The user or group defines who can perform the task.

As the following diagram illustrates, you must have all three elements in order to have a permission.

Note: In this diagram, the gray boxes indicate components that exist in the vCenter Server, and the white boxes indicate components that exist in the operating system where the vCenter Server is running.



Privileges

From the perspective of working with Virtual Storage Console for VMware vSphere, there are two kinds of privileges:

- Native vCenter Server privileges
  These privileges come with the vCenter Server.
- VSC-specific privileges
  These privileges were defined for specific VSC tasks. They are unique to VSC.

Note: To make the this document easier to read, it refers to the vCenter Server privileges as native privileges, and the privileges defined for VSC as VSC-specific privileges. For detailed information about VSC-specific privileges, see *Virtual Storage Console for VMware vSphere Advanced RBAC Configuration*. For information about vCenter Server native privileges, see VMware's *vSphere Security* guide. At the time this document was created, that guide was online at *http://pubs.vmware.com/vsphere-51/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-51-security-guide.pdf*. NetApp follows the VMware recommendations for creating and using permissions.

VSC tasks require both VSC-specific privileges and vCenter Server native privileges. These privileges make up the "role" for the user. A permission can have multiple privileges.

Note: To simplify working with vCenter Server RBAC, VSC provides several standard roles that contain all the required VSC-specific and native privileges to perform VSC tasks.

If you change the privileges within a permission, the user associated with that permission should **log out and then log back in** to enable the updated permission.

vSphere objects

Permissions are associated with vSphere objects, such as the vCenter Server, ESXi hosts, virtual machines, datastores, datacenters, and folders. You can assign permissions to any vSphere object. Based on the permission assigned to a vSphere object, the vCenter Server determines who can perform which tasks on that object.

Users and groups

You can use Active Directory (or the local vCenter Server machine) to set up users and groups of users. You can then use vCenter Server permissions to grant access to these users or groups to enable them to perform specific VSC tasks.

Note: These vCenter Server permissions apply to VSC vCenter users, not VSC administrators. By default, VSC administrators have full access to the product and do not need to have permissions assigned to them.

Users and groups do not have roles assigned to them. They gain access to a role by being part of a vCenter Server permission.

You can assign only one permission to a vCenter user or group. You can, however, set up high-level groups and assign a single user to multiple groups. Doing that allows the user to have all the permissions provided by the different groups. In addition, using groups simplifies the management of permissions by eliminating the need to set up the same permission multiple times for individual users.

Key points about assigning and modifying permissions

There are several key points to keep in mind when you are working with vCenter Server permissions. Whether a Virtual Storage Console for VMware vSphere task succeeds can depend on where you assigned a permission or what actions a user took after a permission was modified.

You only need to set up vCenter Server permissions if you want to limit access to vSphere objects and tasks. Otherwise, you can log in as an administrator. This login automatically allows you to access all vSphere objects.

Note: For detailed information on working with vCenter Server permissions, see the VMware *vSphere Security* guide. At the time this document was created, that guide was online at http://pubs.vmware.com/vsphere-51/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-51-security-guide.pdf. NetApp follows the VMware recommendations for creating and using permissions.

Assigning permissions

Where you assign a permission determines the VSC tasks that a user can perform.

Sometimes, to ensure that a task completes, you must assign the permission at a higher level, such as the root object. This is the case when a task requires a privilege that does not apply to a specific vSphere object (for example, tracking the task) or when a required privilege applies to a non-vSphere object (for example, a storage system).

In these cases, you can set up a permission so that it is inherited by the child entities. You can also assign other permissions to the child entities. The permission on a child entity always overrides the permission inherited from the parent entity. This means that you can assign child entity permissions as a way to restrict the scope of a permission that was assigned to a root object and inherited by the child entity.

Tip: Unless your company's security policies require more restrictive permissions, it is a good practice to assign permissions on the root object (also referred to as the root folder). Then, if you need to, you can restrict those entities that you do not want to have the permission so that you have more fine-grained security.

Permissions and non-vSphere objects

In some cases, a permission applies to a non-vSphere object. For example, a storage system is not a vSphere object. If a privilege applies to a storage system, you must assign the permission containing that privilege to the VSC root object because there is no vSphere object to which you can assign it.

For example, any permission that includes a privilege such as the VSC privilege "Add/Modify/Skip storage systems" must be assigned at the root object level.

Modifying permissions

You can modify a permission at any time.

If you change the privileges within a permission, the user associated with that permission should **log out and then log back in** to enable the updated permission.

Advanced example of using vCenter Server permissions

The privileges you include in a vCenter Server permission determine the role that the Virtual Storage Console for VMware vSphere user has and the tasks associated with that role. In addition, the vSphere object to which you assign the permission also affects the tasks the user can perform. This example illustrates those points.

Note: Depending on your system setup and company's security requirements, you might either log in as administrator and not use vCenter Server RBAC, or you might set permissions on the root object (folder). Setting permissions on the root object normally allows all the child objects to inherit those permissions, unless you place a restriction on a child object to exclude it.

If you plan to use a more restrictive implementation of RBAC, the following example illustrates how assigning permissions can affect which tasks you can complete. This example uses two datacenters (Datacenter A and Datacenter B) that are managed by a single vCenter Server. Users of one datacenter are not allowed to perform tasks in the other datacenter.

For Datacenter A, you create the following vCenter Server permission:

- A user named "Pat"
- The vCenter Server privileges, both VSC-specific and vCenter Server native, required to allow the user to perform rapid cloning
- A managed object within the vSphere inventory (Datacenter A), which has the "Propagate to Child Objects" check box selected

Because the permissions for rapid cloning are assigned to Datacenter A, VSC displays an error message if you attempt to clone a virtual machine from Datacenter B.

If you attempt to clone a virtual machine in Datacenter A, VSC allows you to complete the Rapid Clone Wizard steps. However, when you click **Apply**, the Rapid Clone Wizard disappears without completing the cloning task. The log file includes a message stating that you do not have permission to create a task.

This clone task failed because the permission was applied to Datacenter A instead of the root object (folder). The task required the native vCenter Server privilege "Create Task." Permissions containing the "Create Task" privilege must always be applied at the root object level. During the cloning task, Provisioning and Cloning confirmed that "Pat" had permission to work with a virtual machine in Datacenter A. But, as the clone task continued, Provisioning and Cloning asked the vCenter Server to create a task to track its progress. The vCenter Server rejected this request because user "Pat" did not have permission to create tasks on the root object. This caused the task to fail.

If you had assigned the permission at the root object, the privileges would have propagated down to the child vSphere objects, in this case Datacenter A and Datacenter B. You could have prevented "Pat" from working with a virtual machine in Datastore B by applying a permission restricting "Pat" from accessing Datastore B.

For detailed information on working with vCenter Server permissions, see VMware's *vSphere Security* guide. At the time this document was created, that guide was online at http://pubs.vmware.com/vsphere-51/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-51-security-guide.pdf. NetApp follows the VMware recommendations for creating and using permissions.

Standard roles packaged with VSC for VMware vSphere

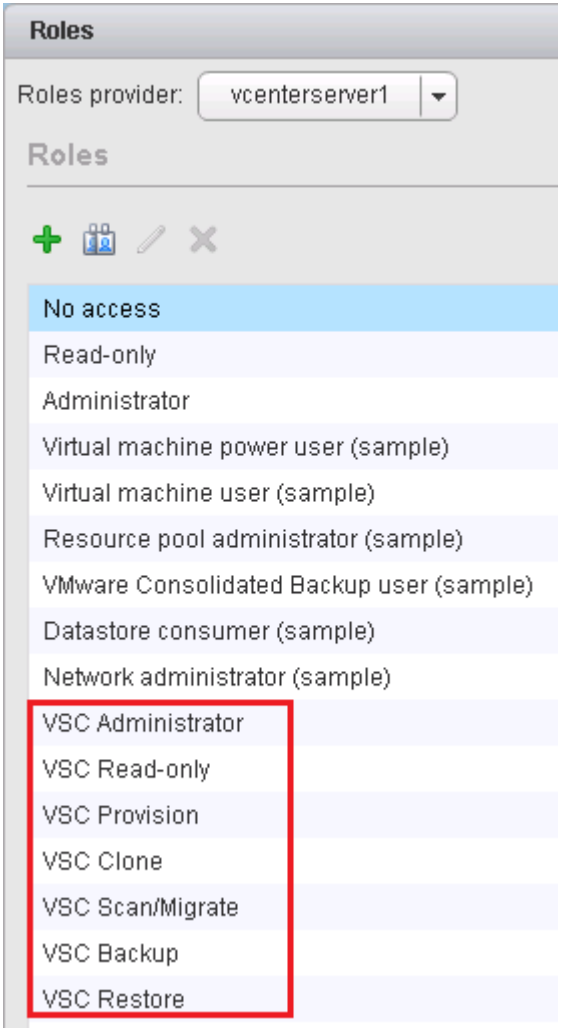
To simplify working with vCenter Server privileges and role-based access control (RBAC), Virtual Storage Console for VMware vSphere provides a set of standard VSC roles that enables users to perform key VSC tasks. There is also a read-only role that allows users to view VSC information, but not perform any tasks.

The standard VSC roles have both the required VSC-specific privileges and the native vCenter Server privileges to ensure that tasks complete correctly. In addition, the roles are set up so that they have the necessary privileges across all supported versions of the vCenter Server.

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

Note: VSC returns these roles to their default values (initial set of privileges) each time you restart the VSC Windows service or modify your installation. If you upgrade VSC, the standard roles are automatically upgraded to work with that version of VSC.

You can see the VSC standard roles when you click **Roles** from the VMware vSphere Web Client Home page.



The roles VSC provides allow you to perform the following tasks:

Role	Description
VSC Administrator	Provides all native vCenter Server and VSC-specific privileges necessary to perform all VSC tasks.
VSC Read-only	Provides read-only access to all of VSC. These users cannot perform any VSC actions that are access controlled.

Role	Description
VSC Provision	Provides all native vCenter Server and VSC-specific privileges necessary to provision storage. The user can perform the following tasks: • Create new datastores • Destroy datastores • View information about storage capability profiles The user cannot perform the following tasks: • Create clones • Reclaim space • Distribute templates
VSC Clone	Provides all native vCenter Server and VSC-specific privileges necessary to clone storage and view information about storage capability profiles. The user cannot perform the following tasks: • Provision storage • Reclaim space • Distribute templates
VSC Scan/Migrate	Provides all native vCenter Server and VSC-specific privileges necessary to scan databases and migrate virtual machines and view information about storage capability profiles. With this role, the user can perform all tasks involving optimizing and migrating storage. The user also has access to the configure privilege.
VSC Backup	Provides all native vCenter Server and VSC-specific privileges necessary to back up vSphere objects (virtual machines and datastores) and view information about storage capability profiles. The user also has access to the configure privilege. The user cannot perform the following task: • Restore storage

Role	Description
VSC Restore	Provides all native vCenter Server and VSC-specific privileges necessary to restore vSphere objects that have been backed up and view information about storage capability profiles. The user also has access to the configure privilege. The user cannot perform the following task: • Back up vSphere objects.

Details about the privileges needed for these roles are included in *Virtual Storage Console for VMware vSphere Advanced RBAC Configuration Guide*.

Product-level privilege required by VSC for VMware vSphere

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

The following information describes the VSC product-level View privilege:

Privilege	Description	Assignment level
View	You can access the VSC GUI. This privilege does not enable you to perform tasks within VSC. To perform any VSC tasks, you must have the correct VSC-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 VSC by clicking the NetApp icon. You can assign the View privilege to another vSphere object level; however, doing that limits the VSC menus that you can see and use. The root object is the recommended place to assign any permission containing the View privilege.

Example of how the View privilege affects tasks in VSC for VMware vSphere

The View privilege allows you to see the Virtual Storage Console for VMware vSphere GUI. Where you assign a permission containing the View privilege determines which parts of the GUI are visible.

Note: Depending on your company's security requirements, you might either log in as administrator and not use RBAC, or you might set permissions on the root object (folder). Setting permissions on the root object normally allows all the child objects to inherit those permissions, unless you place a restriction on a child object.

If you plan to implement RBAC in a more restrictive way, the following example illustrates how assigning a permission containing the View privilege can affect which parts of the GUI you can access. In this example, the following vCenter Server permission is assigned to Datacenter A:

- A user named "Pat"
- Privileges that include the View privilege
- A managed object within the vSphere inventory (Datacenter A), which has the "Propagate to Child Objects" check box selected

If you log in to VSC as user "Pat", the NetApp icon appears. However, if you click the icon, VSC displays an error message. This is because "Pat" only has View permission on Datacenter A. To see the VSC menus and toolbars, you must navigate to Datacenter A and right-click it.

To access the main VSC GUI and avoid an error message when you click on the icon, you must assign any permission containing the View privilege to the root object.

Data ONTAP role-based access control features in VSC for VMware vSphere

Data 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. In Virtual Storage Console for VMware vSphere, Data ONTAP RBAC works with vCenter Server RBAC to determine which VSC tasks a specific user can perform on objects on a specific storage system.

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

Data ONTAP RBAC applies only to accessing storage systems and performing VSC tasks related to storage, such as cloning virtual machines. If you do not have the appropriate Data ONTAP RBAC privileges for a specific storage system, you cannot perform any tasks on a vSphere object hosted on that storage system. You can use Data ONTAP RBAC in conjunction with the VSC-specific privileges to control which VSC tasks a user can perform:

- Monitoring and configuring storage or vCenter Server objects residing on storage
- Provisioning and cloning vSphere objects residing on storage
- Scanning, optimizing, and migrating vSphere objects residing on storage
- Backing up and recovering vSphere objects residing on storage

Using Data ONTAP RBAC with the VSC-specific privileges provides a storage-oriented layer of security that the storage administrator can manage. As a result, you have more fine-grained access control than either Data ONTAP or vCenter Server supports alone. For example, with vCenter Server RBAC, you can allow vCenterUserB, but not vCenterUserA, to provision a datastore on NetApp storage. However, if the storage system credentials for a specific storage system do not support creating storage, then neither vCenterUserB nor vCenterUserA can provision a datastore on that storage system.

When you initiate a VSC task, VSC first confirms that you have the correct vCenter Server permission for that task. If the vCenter Server permission is not sufficient to allow you to perform the task, VSC does not need to check the Data ONTAP privileges for that storage system because you did not pass the initial, vCenter Server security check. As a result, you cannot access the storage system.

If the vCenter Server permission is sufficient, VSC then checks the Data ONTAP RBAC privileges (your Data ONTAP role) associated with the storage system's credentials (the user name and password) to determine whether you have sufficient privileges to perform the storage operations required by that VSC task on that storage system. If you have the correct Data ONTAP privileges, you can access the storage system and perform the VSC task. The Data ONTAP roles determine the VSC tasks you can perform on the storage system.

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

Using both Data 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, VSC 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.

Recommended Data ONTAP roles when using VSC for VMware vSphere

There are several recommended Data ONTAP roles that you can set up for working with Virtual Storage Console for VMware vSphere and role-based access control (RBAC). These roles contain the Data ONTAP privileges required to perform the necessary storage operations executed by the VSC tasks.

There are several ways to create Data ONTAP roles:

- RBAC User Creator for Data ONTAP

NetApp Community Document: RBAC User Creator for Data ONTAP

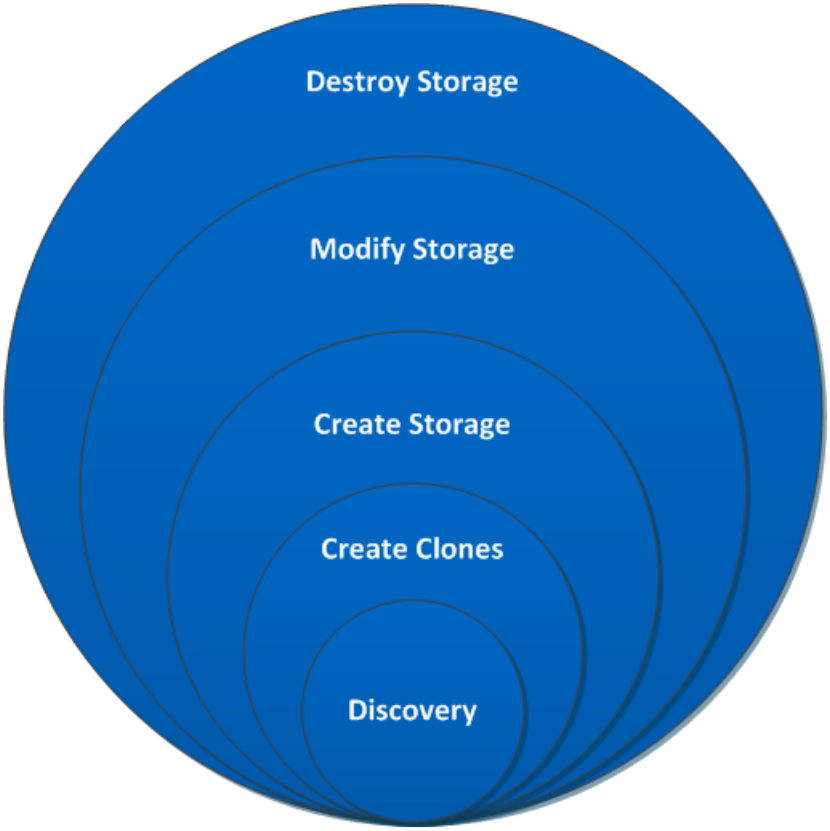
- OnCommand System Manager, which can be downloaded for either Windows or Linux platforms
- The CLI (command-line interface), using the `security login` set of commands

  The *System Administrator's Guide for Clustered Data ONTAP Administrators* contains information about using this command.

Each role has a user name/password pair associated with it. These are the role's credentials. If you do not log in using these credentials, you cannot access the storage operations associated with the role.

As a security measure, the VSC-specific Data ONTAP roles are ordered hierarchically. This means that the first role is the most restrictive role and has only the privileges associated with the most basic set of VSC storage operations. The next role includes both its own privileges and all of the privileges associated with the previous role. Each additional role is less restrictive with regard to the supported storage operations.

The following are some of the recommended Data ONTAP RBAC roles when using VSC. After you create these roles, you can assign them to users who need to perform tasks related to storage, such as provisioning and cloning storage and optimizing and migrating virtual machines.



1. Discovery

The Discovery role enables you to add storage systems.

2. Create Clones
   This role enables you to clone virtual machines. It also includes all of the privileges associated with the Discovery roles.
3. Create Storage
   This role enables you to create storage. It also includes all of the privileges associated with the previous two roles.
4. Modify Storage
   This role enables you to modify storage. It also includes all of the privileges associated with the previous three roles.
5. Destroy Storage
   This role enables you to destroy storage. It also includes all of the privileges associated with all of the above roles.

If you use VSC only to perform backups, then the following Data ONTAP roles are recommended:

1. Discovery
   The Discovery role enables you to add storage systems.
2. Backup-Recover
   This role enables you to back up information on storage systems that you can recover later. It also includes all of the privileges associated with the Discovery role.

If you are using VASA Provider for clustered Data ONTAP, you should also set up a PBM (policy-based management) role. That role will allow you to manage storage using storage policies. This role requires that you also set up the Discovery role.

Each Data ONTAP role that you create can have one user name associated with it. You must log in to the storage system using the appropriate user name/password pair if you want to perform those role-based tasks on the storage system.

To create new users, you must log in as an administrator on storage systems running clustered Data ONTAP or root on storage systems running Data ONTAP operating in 7-Mode.

Details about the privileges needed for these roles are included in *Virtual Storage Console for VMware vSphere Advanced RBAC Configuration Guide*.

How to configure Data ONTAP role-based access control for VSC for VMware vSphere

You must configure Data ONTAP role-based access control (RBAC) on the storage system in order to use it with Virtual Storage Console for VMware vSphere.

From within Data ONTAP, you must perform the following tasks:

- Create the roles.

Note: RBAC User Creator for Data ONTAP

NetApp Community Document: RBAC User Creator for Data ONTAP

- Create a user name/password login (the storage system credentials) in Data ONTAP for each role. You need these storage system credentials to configure the storage systems for VSC. You do this by entering the credentials in VSC. Each time you log in to a storage system using these credentials, you are presented with the set of VSC functions that you set up in Data ONTAP when you created the credentials.

VSC performs an upfront privilege validation for Data ONTAP RBAC when you log in. VSC does not perform the upfront validation if the storage system is directly connected to a Storage Virtual Machine (SVM, formerly known as Vserver) or a vFiler unit. Instead, VSC checks and enforces the privileges later in the task workflow.

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

Requirements for performing tasks in VSC for VMware vSphere

A few requirements impact many of the tasks that you can perform in Virtual Storage Console for VMware vSphere. You should understand requirements for privileges, running simultaneous tasks, and provisioning and cloning operations.

- Unless you log in as administrator, you must have the appropriate RBAC privileges correctly assigned to complete tasks.
- VSC must not be performing another operation on the target virtual machine or datastore that can have a negative impact on the currently executing operation.

  If VSC is performing a task on the target virtual machine or datastore, other tasks are temporarily unavailable.
- (NFS only) Before performing provisioning or cloning operations, you should have enabled the NFS Plug-in for VMware VAAI.

  While not required, installing the plug-in is a best practice because it reduces load from the host and places it on the storage system, which increases cloning efficiency.

Related concepts

Authentication and user management with vCenter RBAC and Data ONTAP RBAC on page 81
VSC for VMware vSphere protects system resources by using lock management on page 19
How VSC for VMware features work with optional plug-ins on page 13
NetApp NFS Plug-in for VAAI installation on page 48

Navigating VSC for VMware vSphere

Virtual Storage Console for VMware vSphere integrates smoothly into the VMware vSphere Web Client and vCenter Server.

To help you distinguish between the VSC features and the vSphere Web Client features, the NetApp blue "N" icon appears in the screens and portlets associated with NetApp features.

You can access VSC tasks from both the vCenter and the Virtual Storage Console portions of the vSphere Web Client. Many of the Actions menus includes a **NetApp VSC** menu.

The Actions menu displays the VSC tasks available based on the object you are interacting with in the vSphere Web Client. For example, if you right-click on a vSphere cluster, the **NetApp VSC** menu displays an option to Provision Datastore.

You can initiate a task by doing any of the following:

- Right-clicking the object to display the Actions menu.
- Selecting the Actions menu from the menu bar.
- Clicking the icon in the menu bar on that page that is associated with the task you want to perform.

You can access data, such as datastores or virtual machines, either by using the navigation panel on the left side of the screen or by clicking an icon. For example, if you want to clone virtual machines, you can either click the VMs and Templates icon on the vSphere Web Client Home page or you can select **vCenter > VMs and Templates**. Both actions take you to the same place.

Many VSC pages provide a filter option. You can use the drop-down list in this option to organize the display to show only the columns with which you want to work. You can also use a text string to filter information. VSC performs a search based on the string and displays the results in a new window. For example, if you enter **aa** in the filter box and there is a datastore named "AA_tester," then VSC displays information on that datastore. To return to your previous window, which lists all the datastores, clear the information in the filter box and press Enter.

If you are new to the vSphere Web Client, here are some tips for navigating through it:

- The Home icon takes you back to the Home view.
- The vCenter icon takes you to the vCenter.
- You can use the back arrow in the navigation pane to return to your previous location.
- The Recent Tasks pane on the right side of the screen lets you monitor the progress of a task that is under way.
- The Work In Progress pane shows you tasks that have been started and paused. To resume a paused task, click its name.
- The Alarms pane lists the Alarms that have occurred.

Working with storage systems

Virtual Storage Console for VMware vSphere provides tools you can use to work with storage systems.

Using VSC, you perform tasks such as the following:

- Have VSC automatically discover storage systems
- Manually add and remove storage systems
- Set up default credentials for VSC to use when it adds storage systems
- Modify the credentials associated with a storage system
- Use VSC's interface to get a quick view of the storage system details

Storage system discovery and credentials overview

Virtual Storage Console for VMware vSphere provides a single mechanism to discover storage systems and to set the storage credentials. The credentials provide the necessary Data ONTAP permissions to enable VSC users to perform tasks using the storage systems.

Before VSC can display and manage storage resources, it must discover the storage systems. As part of the discovery process, you must supply Data ONTAP credentials for your storage systems. These are the privileges (or roles) associated with the user name/password pair assigned to each storage system. These username/password pairs use Data ONTAP role-based access control (RBAC) and must be set up from within Data ONTAP. You cannot change their credentials from within VSC. You can, however, define Data ONTAP RBAC roles using a tool such as "RBAC User Creator for Data ONTAP."

Note: If you log in as an administrator, you automatically have all privileges for that storage system.

When you add a storage system to VSC, you must supply an IP address for the storage system and the username/password pair associated with that system. You can either set up default credentials that VSC will use during its storage system discovery process or manually enter credentials when the storage system is discovered.

Note: If you have vFiler units on storage systems running Data ONTAP 8.*x* software, you must set `httpd.admin.enable` for the vFiler unit in order to enable discovery.

Discovery happens in one of the following ways. In each case, you must supply credentials for any newly discovered storage system.

- When the VSC Windows service starts, VSC begins its automatic background discovery process.
- You click the **Update All** icon or select it from the Actions menu (**Actions > Netapp VSC > Update All**).

Note: IPv6 addresses are not supported.

All of the VSC features require specific permissions to perform tasks. You can limit what users can do based on the credentials associated with the Data ONTAP role. All users with the same storage system user name/password pair share the same set of storage system credentials and can perform the same operations.

Default credentials simplify administrating storage systems

You can use Virtual Storage Console for VMware vSphere to set default credentials for storage systems, hosts, and virtual machines. Setting default credentials that are valid for the storage system means that you do not need to manually enter credentials each time VSC adds a storage system.

For example, when VSC discovers a new storage system, it attempts to log in using the default credentials. If the login fails, the storage system status is set to Authentication Failure, and you must enter credentials manually.

You can set the default credentials by clicking **Configuration > Set Default Credentials** from the Virtual Storage Console Home page. VSC displays a pop-up box with tabs to let you set credentials for the different objects.

If you change the default credentials and select **Update All**, VSC uses the new credentials and attempts to log in to any storage system that has a status of either "Authentication Failure" or "SSL is not configured".

Specifying default credentials

You can use Virtual Storage Console for VMware vSphere to create default credentials for a storage system, host, and virtual machine.

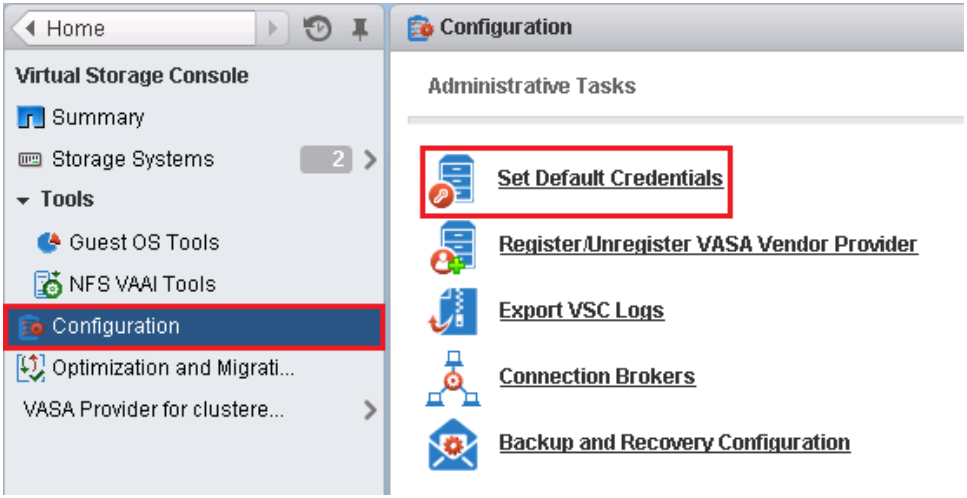
About this task

When you set up default credentials, VSC uses them to attempt to log into a storage system it has just discovered.

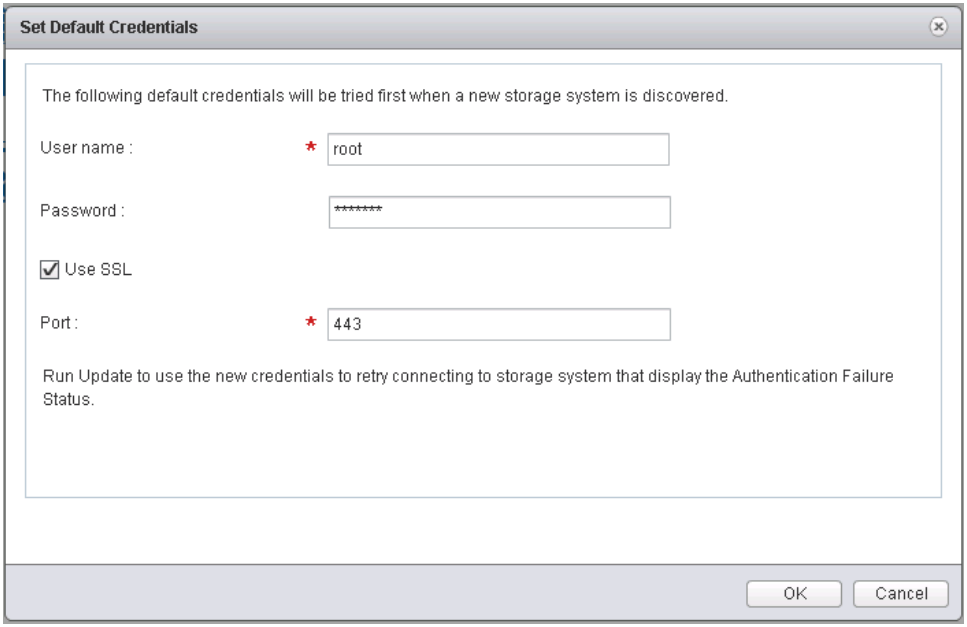
If the default credentials do not work, you will need to manually log in.

Steps

1. From the Virtual Storage Console **Home** page, click **Configuration > Set Default Credentials**.



2. In the **Set Default Credentials** pop-up box, enter the credentials for the storage system.



Storage system field	Explanation
User name/password	Storage controller credentials are assigned in Data ONTAP based on the user name/password pair. This can be the root account or a custom account that uses role-based access control (RBAC). You cannot use VSC to change the roles associated with that user name/password pair. To do that, you must use a tool such as "RBAC User Creator for Data ONTAP."
Use SSL	Check this box to enable Secure Sockets Layer (SSL).
Port	The default management port number is 443 if the SSL box is checked and 80 if it is not checked. These are the Data ONTAP defaults. If you toggle the SSL check box, the port number switches between 443 and 80. You can specify a different port number. If you do that, then toggling the SSL check box only changes the SSL state in the dialog box.

3. After you enter the information, click OK.

After you finish

If you updated the storage system credentials because a storage system reported Authentication Failure Status, select **Update Hosts and Storage Systems**, which is available from the **Actions > NetApp VSC** menu. When you do this, VSC tries to connect to the storage system using the new credentials.

Related tasks

Discovering storage systems and hosts on page 103

Tunneled vFiler units and SVMs discovered automatically

Virtual Storage Console for VMware vSphere automatically supports vFiler and Storage Virtual Machine (SVM, formerly known as Vserver) tunneling for the storage systems. You do not need to manually add these vFiler units and SVMs.

When you enter information for a cluster administrative LIF or vfiler0, VSC discovers all the subordinate vFiler units and SVMs.

If you are using VSC's backup and restore features, there are certain environments where these features can only access the physical storage system, not the vFiler unit, for communication on a storage network. You need to have vFiler tunneling enabled in order to use the backup and restore features to create Snapshot copies.

Enabling discovery and management of vFiler units

If you are using Data ONTAP 8, you must set the `httpd.admin.enable` option for vFiler units in order to enable discovery and management with the Virtual Storage Console for VMware vSphere.

About this task

You do not need to perform this task if your vFiler units were created with Data ONTAP 7.x.

Steps

1. From the storage system, enter the following command to switch to a particular vFiler context:

   `vfiler context *vfiler_name*`

2. Enter the following command in the vFiler context to set the required option that enables discovery in VSC:

   `options httpd.admin.enable on`

3. Repeat these steps for each vFiler unit you want to manage using VSC.

Enabling discovery and management of vFiler units on private networks

If vFiler units are isolated in private networks to which Virtual Storage Console for VMware vSphere has no network connectivity, you must manually add the pFiler to VSC.

Before you begin

The VSC server must have network connectivity to the parent of the vFiler.

Steps

1. You can add a storage system using either the **Add** icon or the **Add Storage System** menu option:

Starting location	Action
Virtual Storage Console Home page	**a.** Click **Storage** **b.** Click the **Add** icon
VMware vSphere Web Client Home page	**a.** Click the **Storage** icon **b.** Select a datacenter **c.** Click the **Actions > NetApp VSC > Add Storage System**

2. In the **Add Storage System** pop-up box, enter the management IP address and credentials for the pFiler and then click **OK**.

Result

Any vFiler units belonging to the parent of the vFiler that provide storage to ESX hosts are discovered by VSC.

Discovering storage systems and hosts

When you first run Virtual Storage Console for VMware vSphere in a VMware vSphere Web Client, it discovers ESX and ESXi hosts, their LUNs and NFS exports, and the NetApp storage systems that own those LUNs and exports. You must then provide the storage system credentials.

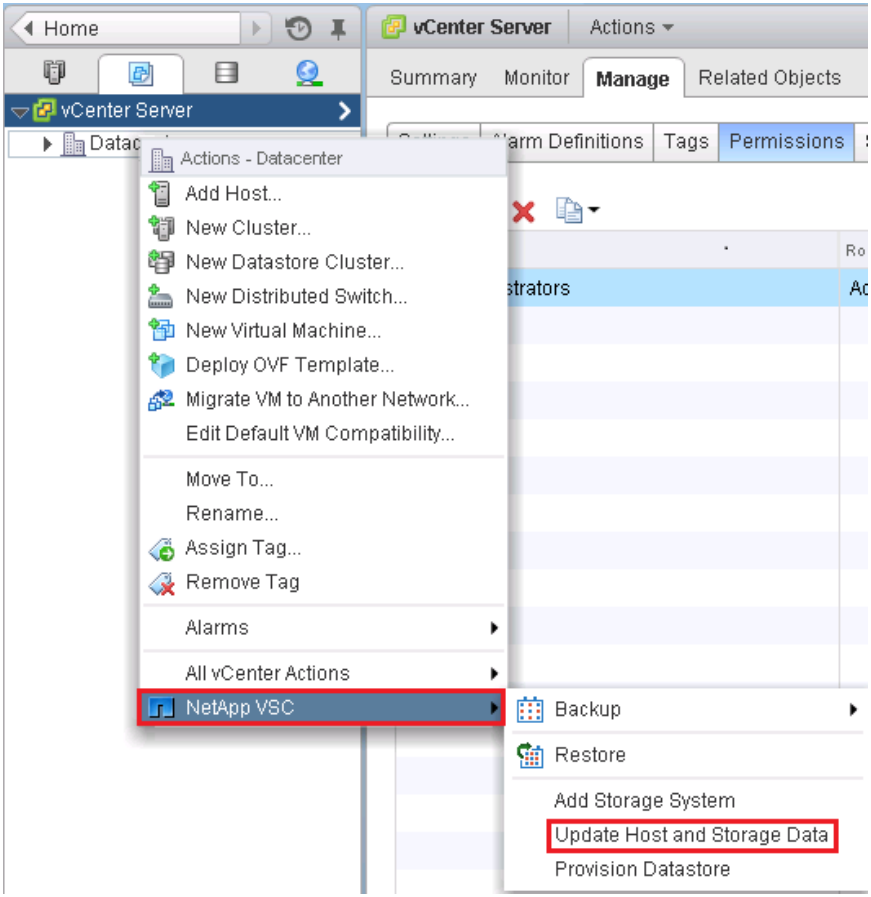
About this task

You can discover new storage systems or update information on them to get the latest capacity and configuration information at any time.

The discovery process also collects information from the ESX and ESXi hosts managed by the vCenter Server. Make sure all ESX and ESXi hosts are shown as powered on and connected.

Steps

1. From the the vSphere Web Client **Home** page, select **vCenter**.
2. Right-click a datacenter and select **Actions > NetApp VSC > Update Host and Storage Data**.



3. VSC displays a **Confirm** dialog box that warns you that this operation can take a long time. Click **OK**.
4. Right-click any discovered storage controllers that have the status Authentication Failure and select **Modify**.
5. Fill in the information in the **Modify Storage System** dialog box.

After you finish

After discovery is complete, use VSC to configure ESX or ESXi host settings for any hosts displaying an Alert icon in the Adapter Settings, MPIO Settings, or NFS Settings columns.

Refreshing the storage system display

You can use the update feature provided by Virtual Storage Console for VMware vSphere to refresh the information about storage systems and force VSC to discover storage systems. This can be

especially useful if you changed the default credentials for the storage systems after receiving an authentication error.

About this task

You should always perform an update operation if you changed the storage system credentials after a storage system reported an Authentication Failure Status. During the update operation, VSC tries to connect to the storage system using the new credentials.

Depending on your system setup, this task can take a long time to complete.

Steps

1. Go to the **Storage** page by clicking **Storage** from either the navigation pane of the Virtual Storage Console **Storage** page or the icon on the VMware vSphere Web Client **Home** page.
2. Start the update:

Location	Click ...
Virtual Storage Console	The **Update All** icon.
vCenter	**Actions > NetApp VSC > Update Host and Storage Data**

3. Click OK at the Confirm dialog box.
4. Click OK at the Success Message dialog box.

   This operation works in the background.

Removing storage systems from VSC

You can remove a skipped or unmanaged storage system that is not attached to a host. When you remove a storage system, it no longer appears in the Virtual Storage Console for VMware vSphere display.

About this task

If a storage system has storage mapped to an ESX or ESXi host managed by VSC and you attempt to remove that storage system, VSC displays an error message and does not remove the storage system. You can only remove storage systems that are not attached to hosts.

Step

1. You can remove a storage system by clicking **Storage** from either the VSC **Home** page or the VMware vSphere Web Client **Home** page.

Starting location	Action
Virtual Storage Console Home page	**a.** Click **Storage** **b.** Right-click a storage system and select **Actions > NetApp VSC > Delete**
VMware vSphere Web Client Home page	**a.** Click the **Storage** icon **b.** Right-click a datastore and select **Actions > NetApp VSC > Destroy**

The action VSC takes depends on whether the storage system is attached to a host:

If the storage system is ...	VSC...
Not attached to host	Removes the storage system
Attached to a host	Displays an error message and does not change the storage system

Correcting storage system names displayed as "unknown"

If Virtual Storage Console for VMware vSphere displays a storage system name as "unknown," you can modify the credentials and add the management IP address of the storage system in the Modify Storage System pop-up box.

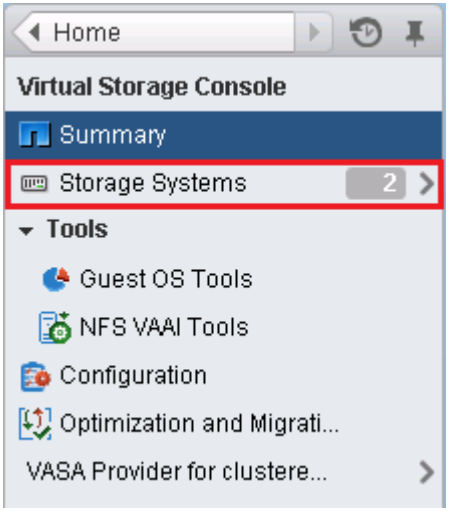
About this task

An "unknown" name can occur if an NFS datastore is mounted over a private network.

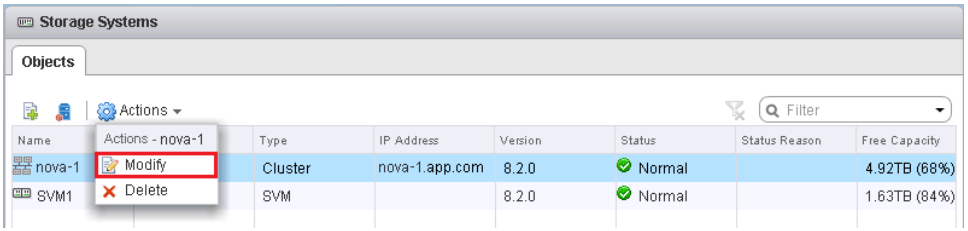
If you are running clustered Data ONTAP and working with NFS datastores that are mounted using an NFS data LIF, this issue can occur with either a private network or a public network.

Steps

1. From the Virtual Storage Console **Home** page, click **Storage Systems**.



2. Right-click the storage system shown as "unknown" and select **Modify Storage System**.



3. Enter the management IP address of the storage system and the storage system credentials in the **Modify storage system -unknown-** pop-up box.

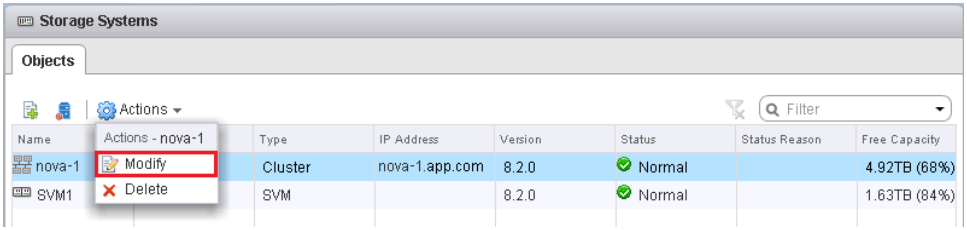
   VSC must have network connectivity to the management port you specify.

Managing settings for volumes

You can specify advanced settings that apply when you provision new volumes on the storage system. These settings include features such as enabling thin provisioning and deleting a volume when the last LUN contained in it is deleted.

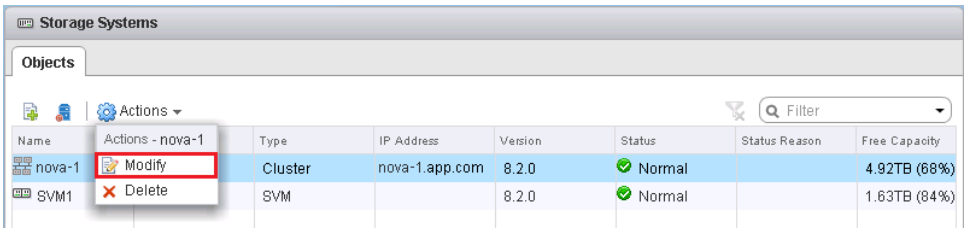
Steps

1. From the Virtual Storage Console **Home** page, click **Storage Systems**.
2. Right-click on a the storage system and select **Modify** from the Actions menu.



3. In the **Modify Storage System** pop-up box, click the **Provisioning Options** tab.

   If storage system properties have been locked to prevent changes, click **Enable Editing**. In the resulting dialog box, enter the username and password for that storage system. Virtual Storage Console for VMware vSphere will not let you change the settings until you enter this information.



4. After you have enabled editing, check the boxes next to the advanced options and enter information to modify the FlexVol efficiency settings to match those on the LUN being deployed.

   Note: If a thin provisioned LUN is deployed into a FlexVol with volume autogrow or snapshot autodelete disabled, it is possible to over-commit the LUN to the volume. This creates an out-of-space condition.

Option	Explanation
Create a new volume for a new LUN	Selecting this option creates a FlexVol with the same name as the LUN. If a volume with that name already exists, VSC appends a number to the volume name; for example: `Volname01`
Reserve space for volumes that contain thin provisioned LUNs	Checking this results in having a thin LUN in a thick volume when a thin LUN is chosen.
Thin provision volume clones	Sets the space reservation policy to thin provisioning for clones created from this volume.
Delete a volume if the last LUN in it has been deleted	Destroys the volume when the last LUN on it is deleted.
Buffer space between volume and LUN (GB)	Specifies the amount of additional capacity in a volume that contains a LUN-based datastore.

5. Click **OK** when you finish.

MultiStore vFiler units are displayed differently

Virtual Storage Console for VMware vSphere displays vFiler units differently than physical storage controllers.

When you have a vFiler unit created with the optional MultiStore feature of Data ONTAP software, VSC displays the following information:

- The hostname displays a "MultiStore" prefix to identify vFiler units.
- The **Supported Protocols** column reports the storage protocols actually in use by ESX and ESXi hosts instead of the protocols licensed for the storage controller.
- The **Alert** icon in the **Status** column means that the vFiler unit does not respond to VSC. The **Normal** icon means that VSC is able to communicate with the vFiler unit.
- No detailed status is returned for vFiler units. The **Status Reason** column displays `This controller is a MultiStore vFiler unit`. You can connect to the physical controller that owns the vFiler unit to get more status information.
- No aggregate information is displayed for vFiler units.
  Direct vFiler units and direct Storage Virtual Machines (SVMs) do not have aggregates to display.

Differences between direct connections to SVMs and to cluster-management LIFs

Virtual Storage Console for VMware vSphere supports connecting a storage system directly to either a Storage Virtual Machine (SVM, formerly known as Vserver) or a cluster-management LIF. When the storage connects directly to an SVM, not all of the VSC features are supported. To use all the features, you must connect the storage to a cluster-management LIF.

VSC does not provide the following features when the storage system connects directly to an SVM:

- **Upfront validation of Role-Based Access Control (RBAC)**
  While RBAC is fully supported, VSC does not perform the initial privilege validation on storage that is directly connected to an SVM.
- **NFS path checking**
  When you are using clustered Data ONTAP and a cluster-management LIF, VSC can query the storage system to determine whether that storage system is using a direct or indirect path. VSC then reports this information and supplies information that you can use to set up a direct path. Better performance is normally seen when direct paths are used. If a storage system connects directly to an SVM, VSC cannot query the storage system to determine the path.
- **Reports on space that is shared by volumes using data deduplication**
  VSC is not able to check the space shared by volumes that have data deduplication enabled when the storage system is directly attached to an SVM.

- **Load-sharing mirrors updates**
  VSC cannot update the mirror if you use load-sharing mirrors for your SVM's root volume.
- **EMS logging**
  VSC cannot perform EMS logging when the storage system is directly attached to an SVM.

These features are supported when the storage system connects to a cluster-management LIF.

Direct path access and NFS datastores

When you are running clustered Data ONTAP, it is possible for a client to access a data LIF with an indirect data path to a FlexVol. Indirect data paths can negatively affect I/O performance and should be corrected. Virtual Storage Console for VMware vSphere provides tools to scan for direct and indirect NFS paths and provide you with the information you need to manually correct paths.

An indirect path can occur when a data LIF is bound to a different physical node than the one that owns the exported FlexVol. The NFS virtual client does not have the path selection intelligence that is native to physical clients. In order to have a direct data path, the client must access a data LIF that is local to the node that owns the exported FlexVol.

VSC monitors which LIFs NFS is using to access the volume. You can see whether a LIF uses a direct data path or an indirect data path by clicking the **NAS** tab in the Related Objects page for a storage system and viewing the Data Path Access column. This column displays the path setting as Direct (green check), Indirect (red exclamation point (!)), N/A, or (unknown).

If the path setting is indirect, you can right-click that row and select the **View Direct Data Path Choices** option. This option displays the **Direct Data Path Choices** pop-up, which contains a list of ports using direct paths to access data.

Note: VSC does not check these ports to ensure that they are connected to the network. You must do that manually.

Anytime the data path access changes, either to direct from indirect or to indirect from direct, VSC writes the path information to a log file.

If a direct Storage Virtual Machine (SVM) connection is made, VSC cannot query the storage controller to determine the path.

An N/A (not applicable) entry indicates a path to a storage controller running Data ONTAP operating in 7-Mode, so there is no issue about whether the path is direct.

An unknown path occurs if the discovery data is incomplete.

Changing NFS data paths to direct access

If you have a cluster node that is accessing a data LIF with an indirect data path, you can change the path to one that is direct. Virtual Storage Console for VMware vSphere provides information about

the paths; however, the task of moving the path must be performed by a storage administrator using either the storage system console or a NetApp tool such as System Manager.

Before you begin

Only a storage administrator should change the path.

About this task

The need to change paths only occurs when your clustered Data ONTAP configuration has an NFS datastore using a remote data LIF that is bound to a different physical node than the one that owns the exported FlexVol.

Steps

1. From the Virtual Storage Console **Home** page, click **Storage** > ***<storage system name>*** > **Related Objects** > **NAS**.
2. Right-click a row that has an indirect data path (shown as Indirect) and select the **View Direct Data Path Choices** option.

   This option displays the **Direct Data Path Choices** pop-up, which contains a list of ports to data paths providing direct access. You cannot use this window to change the path, but you can use it to get information about the available ports.
3. Manually check to make sure the port you want to use is connected to the network.

   VSC displays the ports without checking their network connectivity. If you try to use a port that is not connected to the network, your datastore will go offline.
4. After you have confirmed that the path you want to use is connected to the network, collect the information displayed in the **Direct Data Path Choices** pop-up and give it to a storage administrator.

   The **Direct Data Path Choices** pop-up contains all the information a storage administrator needs to move the LIF.

   To create a data path with direct access, you must have the correct credentials.

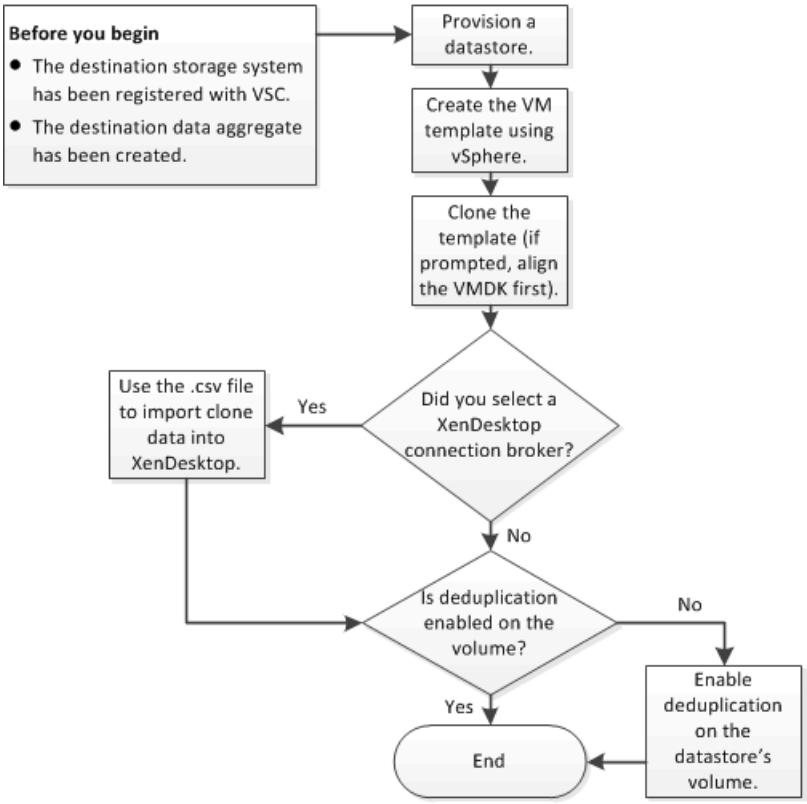
   Note: If multiple datastores are using that LIF, moving the LIF will cause the other datastores to have data paths with indirect data access.
5. Use either the storage system console or a NetApp tool such as System Manager to change the path.

   Note: Whenever the path value changes, VSC writes the information to a log file.

Deploying virtual machines on NetApp storage

You can use Virtual Storage Console for VMware vSphere to deploy virtual machines by provisioning datastores and then rapidly cloning the virtual machines from a template into the provisioned datastores.

The following workflow shows how you can provision datastores using the Datastore Provisioning wizard before using the Create Rapid Clones wizard to clone virtual machines. This workflow is beneficial because the Datastore Provisioning wizard allows you to specify a storage capability profile, which ensures that consistent Service Level Objectives (SLOs) are maintained and simplifies the provisioning process, if you use VASA Provider for clustered Data ONTAP.



Related concepts

VASA Provider for clustered Data ONTAP configuration on page 63

Provisioning datastores

Provisioning a datastore creates a logical container for your virtual machines and their VMDKs. You can provision a datastore and attach it to a single host, to the hosts in a cluster, or to the hosts in a datacenter by using the Datastore Provisioning wizard.

Before you begin

- To provision NFS datastores to vFiler units, you must have added the default vFiler unit (vFiler0) to Virtual Storage Console for VMware vSphere.
- To provision a datastore to a Storage Virtual Machine (SVM, formerly known as Vserver) that is directly connected to VSC, you must have added the SVM to VSC using a user account that has the appropriate privileges, not the default vsadmin user account or vsadmin role.
- If you use NFS or iSCSI and the subnet is different between your ESX hosts and your storage system, NFS or iSCSI settings in the VSC preferences file must include the ESX host subnet masks.

  For more information, see *Enabling datastore mounting across different subnets* on page 78.

About this task

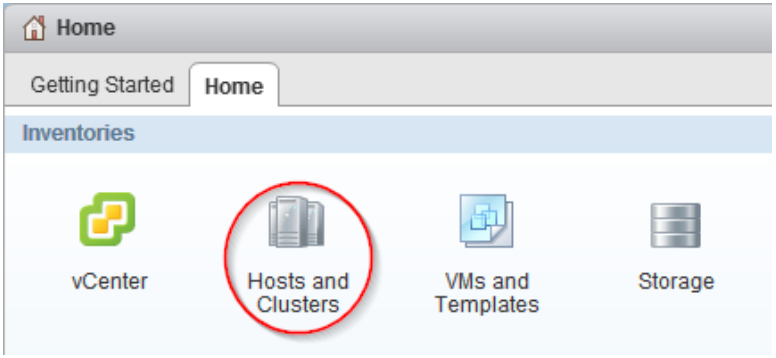
VSC enables you to provision datastores from wizards other than the Datastore Provisioning wizard (for example, from the Create Rapid Clones wizard); however, using the Datastore Provisioning wizard is beneficial because it allows you to specify a storage capability profile, which ensures that consistent Service Level Objectives (SLOs) are maintained and simplifies the provisioning process.

VSC creates a datastore on an NFS volume or a LUN. The following happens when you provision a datastore:

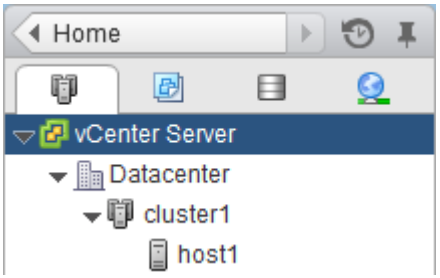
- For an NFS datastore, VSC creates an NFS volume on the storage system and updates export policies.
- For a VMFS datastore, VSC creates a new volume (or uses an existing volume, if you selected that option), and creates a LUN and an igroup.

Steps

1. From the vSphere Web Client **Home** page, click **Hosts and Clusters**.



2. In the navigation pane, expand the datacenter where you want to provision the datastore.



3. Specify the hosts to which you want to mount the datastore:

To make the datastore available to...	Do this...
All hosts in a datacenter	Right-click the datacenter and select **NetApp VSC** > **Provision Datastore**.
All hosts in a cluster	Right-click a cluster and select **NetApp VSC** > **Provision Datastore**.
A single host	Right-click a host and select **NetApp VSC** > **Provision Datastore**.

4. Complete the pages in the **Datastore Provisioning** wizard to create the datastore.
   a. In the **Name and type** page, specify a datastore name, datastore type, and select a storage capability profile, if desired.

      You can specify an existing storage capability profile that the wizard will use when defining the type of storage that you need for your virtual machines. The storage capability profile determines the following storage features: availability, disaster recovery, performance, protocol, and space efficiency. Storage capability profiles are available only if you installed and registered the VASA Provider for clustered Data ONTAP. You can select a default storage capability profile, which ships with the VASA Provider, a profile that you created, or a profile that was auto-generated. To provision a datastore without a storage capability profile, select **None**.
   b. In the **Storage system** page, specify the storage system that you want to use for the datastore.

Note: When connecting directly to an SVM, the provisioning operation might begin, but later fail due to insufficient privileges for the SVM user. SVM privileges are not visible to VSC prior to the operation. If the operation fails, you need to modify the privileges for that SVM user. You can check VSC logs for messages that identify the failed command. An alternative is to use the "RBAC User Creator for Data ONTAP" tool.

c. In the **Details** page, specify details about the datastore that you want to create.

Most of the fields on this page are self-explanatory. The following table describes fields for which you might need guidance:

Field	Description
Thin provision	Allocates space on the volume when data is written, which allows you to provision more storage than is currently available. If disabled, space is reserved immediately. You must closely monitor the available space in the containing aggregate because thin provisioning can oversubscribe the available space. In an NFS configuration, you can enable auto grow to automatically expand the datastore when space is needed. Make sure that the value you specify for auto grow is larger than the size of the datastore.
Aggregate	Defines the aggregate on which you want to create a new volume. If you selected an SVM that is directly connected to VSC, striped aggregates appear as available; however, they are not supported. Provisioning to a striped aggregate will fail.
Volume	Specifies the volume on which you want to create the datastore. For clustered Data ONTAP, you should not create a datastore in the Storage Virtual Machine (SVM) root volume.
Auto grow	(NFS only) Automatically expands the datastore by the specified increment when space is needed, up to the size limit. This size limit you specify must be larger than the existing datastore.
Datastore cluster	Adds the datastore to a cluster if the Storage Distributed Resource Scheduler (SDRS) feature is enabled on the vCenter Server. Do not mix datastores with varying offsets in the same cluster and do not mix optimized and non-optimized datastores.

d. In the **Ready to complete** page, Review the summary of your selections and click **Finish**.

Result

VSC creates the datastore.

After you finish

Add virtual machines to the datastore.

Related concepts

Storage system discovery and credentials overview on page 98
VASA Provider for clustered Data ONTAP and VSC for VMware vSphere on page 14
How to configure Data ONTAP role-based access control for VSC for VMware vSphere on page 94

Related tasks

Creating and editing storage capability profiles on page 65
Mapping storage to storage capability profiles on page 71

Cloning virtual machines from a template

Setting up virtual machines can be a lengthy process. If you need to deploy multiple identical virtual machines, you can save time by setting up a single virtual machine as the template and then rapidly cloning virtual machines from that template.

Before you begin

- You should have created a virtual machine template using VMware vSphere.
- You should have installed the NFS Plug-in for VMware VAAI.
  While not required, installing the plug-in is a best practice because it reduces load from the host and places it on the storage system, which increases cloning efficiency.

About this task

Cloning performance is affected by many factors, including the vCenter Server hardware configuration, the number and hardware configuration of the ESX/ESXi hosts, and the current load on the vCenter Server and the hosts.

Performance can degrade if you request a large number of clones in a single operation. If you need to create a large number of clones, consider whether you should perform two cloning operations instead of one. For example, instead of requesting 2,000 clones in each operation, you might perform two operations that each request 1,000 clones each.

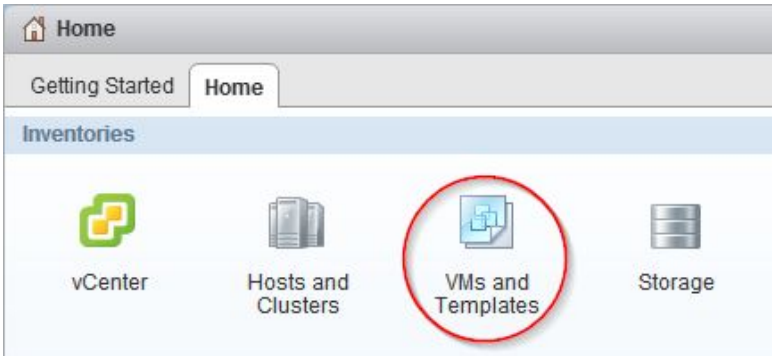
Steps

1. Power down the virtual machine template.

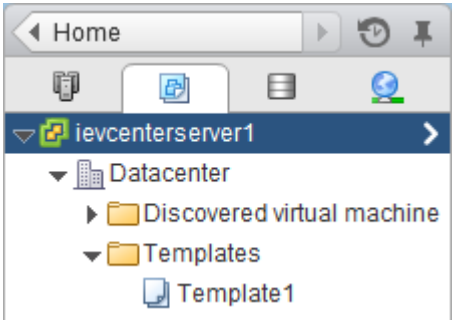
   Powering down the virtual machine is recommended because it enables VSC to check the virtual machine's alignment and perform the cloning process faster. Checking the alignment is important because you should not clone a functionally aligned or misaligned virtual machine. Doing so can result in misaligned clones.

   For more information about functionally aligned and misaligned virtual machines, see *Optimizing I/O performance with online alignment and migration of virtual machines* on page 122.

2. From the vSphere Web Client **Home** page, click **VMs and Templates**.



3. In the navigation pane, expand the datacenter that contains the virtual machine template.



4. Right-click the virtual machine template and select **NetApp VSC > Create Rapid Clones**.

   If VSC warns you that the virtual machine is misaligned or functionally aligned, take the virtual machine offline and use a tool like VMware vCenter Converter to fix the VMDK alignment before you proceed.

   Note: If you do not fix the alignment of a functionally aligned virtual machine, the clones can be misaligned if the destination datastores are not optimized for the VMDK layout of the clones.

5. Complete the pages in the **Create Rapid Clones** wizard to clone the virtual machines.

   a. In the **Clone destination** page, select a destination for the clones (a host, host cluster, or datacenter) and a folder to hold the clones (the default is no folder).

      If you choose a cluster or datacenter, VSC spreads the virtual machines evenly across the hosts.

   b. In the **Clone folder** page, select a folder for the clones.

      Tip: You can create folders on the VMs and Templates page using vCenter actions.

      Note: This page appears if you chose the **Select a folder** option in the Clone destination page.

c. In the **Disk format** page, select a disk format for the clones.

   If you choose the thin provisioned format or the thick format, the wizard warns you that a vSphere clone operation might be required, which can take longer.

d. In the **Virtual machine details** page, specify details about the virtual machine clones.

   Most of the fields on this page are self-explanatory. The following table describes fields for which you might need guidance:

Field	Description
Number of virtual processors	Specifies the number of virtual CPUs for the virtual machines.
Upgrade hardware version?	Upgrades the hardware version of the virtual machine clone if the destination host supports a later version.
Connection broker version	Automatically imports clone data into a VMware View Server or creates a `.csv` file that you can import into Citrix XenDesktop.
Customization specification	Applies a VMware specification to the new virtual machines. Refer to your VMware documentation for information about customization specifications.
Stagger powering on the virtual machines	Staggers the start up of virtual machines to avoid overwhelming your system. You should select this option if you have a large number of virtual machines. The number of virtual machines to start per minute depends on your system environment. **Note:** If a problem prevents VSC from starting some of the virtual machines, the delay could result in VSC powering on a large number of virtual machines at once. For example, if you specify 10 virtual machines per minute and the start is delayed by five minutes, VSC starts 50 virtual machines at once. After the delay, VSC starts the specified number of virtual machines per minute.

e. In the **Storage system details** page, select the storage system where you want to provision the clones.

f. In the **Datastore options** page, choose basic mode or advanced mode to specify the datastore options.

   The advanced mode is a good choice if you want to distribute configuration files and VMDK files across multiple datastores.

g. In the **Datastore details** page, select existing datastores or create new datastores for the clones.

   Most of the fields on this page are self-explanatory. The following table describes fields for which you might need guidance when you create new datastores:

Field	Description
Number of datastores	Specifies the number of datastores to create for the clones. The maximum is 256. The number of clones must be evenly divisible by the number of datastores.
Thin provision	Allocates space on the volume when data is written, which allows you to provision more storage than is currently available. If disabled, space is reserved immediately. You must closely monitor the available space in the containing aggregate because thin provisioning can oversubscribe the available space. In an NFS configuration, you can enable auto grow to automatically expand the datastore when space is needed. Make sure that the value you specify for auto grow is larger than the size of the datastore.
Size (GB)	Specifies the size per datastore.
Aggregate	Defines the aggregate on which you want to create a new volume. If you selected an SVM that is directly connected to VSC, striped aggregates appear as available; however, they are not supported. Provisioning to a striped aggregate will fail.
Volume	Specifies the volume on which you want to create the datastore. For clustered Data ONTAP, you should not create a datastore in the Storage Virtual Machine (SVM) root volume.
Auto grow	(NFS only) Automatically expands the datastore by the specified increment when space is needed, up to the size limit. This size limit you specify must be larger than the existing datastore.
Datastore cluster	Adds the datastore to a cluster if the Storage Distributed Resource Scheduler (SDRS) feature is enabled on the vCenter Server. Do not mix datastores with varying offsets in the same cluster and do not mix optimized and non-optimized datastores.

h. In the **Connection broker** page, specify the VMware view or Citrix XenDesktop connection broker to which you want to import clone data.

   If your connection broker does not appear, you must first add it by going to **Virtual Storage Console > Configuration > Connection Brokers**.

   Note: This page appears if you chose a connection broker version in the Virtual machine details page.

i. In the **Ready to complete** page, Review the summary of your selections and click **Finish**.

Result

VSC creates the virtual machine clones and creates a `.csv` file that includes details about the cloning process. The file, named `import_generic_`*`timestamp`*`.csv`, is created here: *`VSC_install_dir`*`\etc\kamino\exports`

If you chose a VMware View connection broker, VSC automatically imports clone data into the VMware View Server.

If you chose a XenDesktop connection broker, VSC creates a `.csv` file that you can use to import into XenDesktop. The file, named `xenDesktop_`*`timestamp`*`.csv`, is created here: *`VSC_install_dir`*`\etc\kamino\exports`

After you finish

If you chose a XenDesktop connection broker, use the `.csv` file with the Citrix Access Management Console (XenDesktop 4) to create a new desktop group or with Desktop Studio (XenDesktop 5) to create or modify an existing catalog.

Related concepts

How VSC for VMware features work with optional plug-ins on page 13
NetApp NFS Plug-in for VAAI installation on page 48

Increasing storage efficiency by enabling deduplication

Deduplication is a Data ONTAP feature that reduces physical storage space by eliminating duplicate data within a volume. Deduplication enables virtual machines to share the same common data in a datastore, similar to how they share system memory. You should enable deduplication if it is not enabled.

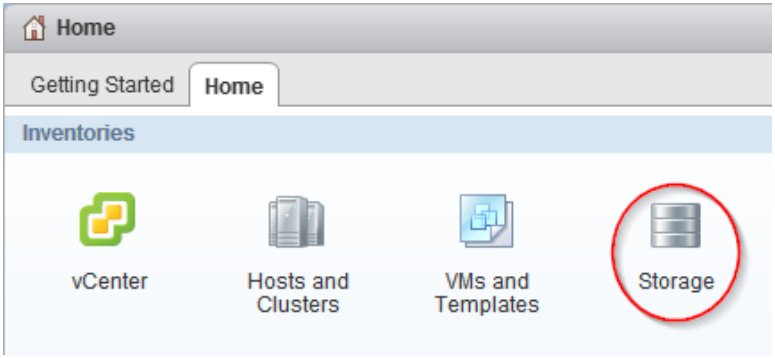
About this task

When Virtual Storage Console for VMware vSphere creates a new volume for a datastore, it enables deduplication by default. If you created the volume through Data ONTAP or OnCommand System Manager, deduplication is not enabled by default. Enabling deduplication is a best practice.

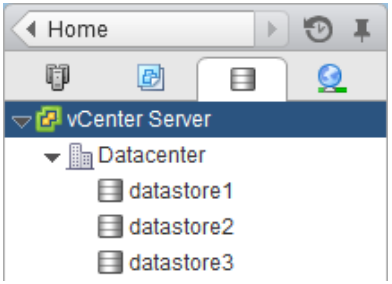
For more information about deduplication, refer to the *Storage Management Guide* for your version of Data ONTAP.

Steps

1. From the vSphere Web Client **Home** page, click **Storage**.



2. In the navigation pane, expand the datacenter that contains the datastore.



3. Select the datastore.
4. Click the **Summary** tab if it does not automatically display.
5. In the **Deduplication Details** pane, view the **State** field to determine whether deduplication is enabled or disabled.

6. If deduplication is disabled, at the bottom of the **Deduplication Details** pane, click **Enable**.

   VSC enables deduplication on the volume. Deduplication runs daily at midnight.
7. Optional: To start deduplication immediately, click **Start**.

After you finish

You can view the Volume Space Saving field to identify the percentage and amount of storage that deduplication saved and the Volume Space Shared field to identify the amount of shared data.

Optimizing performance by aligning the I/O of misaligned virtual machines non-disruptively

Virtual Storage Console for VMware vSphere can scan your datastores to determine the alignment status of virtual machines. You can then use VSC to functionally align the I/O to certain misaligned virtual machines without having to power them down.

About this task

Online alignment is a good choice for virtual machines that you cannot take offline. When possible, you should take the virtual machine offline and physically align the VMDK using a tool such as VMware vCenter Converter.

Steps

1. Scan datastores to determine the alignment status of virtual machines on page 122
2. Check the alignment status of virtual machines on page 123
3. Align the I/O to any misaligned virtual machines on page 125

Related concepts

Methods for migrating virtual machines on page 17

How VSC for VMware vSphere optimizes I/O performance of misaligned virtual machines on page 17

Scanning datastores to determine the alignment status of virtual machines

You should periodically scan datastores to identify whether any of your virtual machines are misaligned. A misaligned virtual machine can negatively affect I/O performance.

About this task

- It is a good practice to scan datastores during non-critical production times.
  The time required to perform a scan can increase as more virtual machines are scanned.
- Virtual Storage Console for VMware vSphere uses VMware snapshots to scan virtual machines that reside in VMFS datastores and then deletes the snapshots when they are no longer needed.

Steps

1. From the vSphere Web Client **Home** page, click **Virtual Storage Console**.

2. In the navigator pane, click **Optimization and Migration**.
3. Initiate a scan of the datastores:

To...	Do this...
Schedule recurring scans	**a.** Click **Global Scan Schedule** and set a schedule for the scan. You should schedule the scans during non-critical production times. **b.** Click **OK**. **c.** To add or remove datastores from the global scan, select a datastore in the datastores table (the table at the top of the Optimization and Migration page) and click **Exclude** or **Include**.
Initiate a one-time scan	**a.** Choose to scan all datastores or specific datastores: • To scan all datastores, click **Scan All**. • To scan one or more datastores, select the datastores and click **Scan selected**. **b.** Click **OK** to confirm the scan.

Result

VSC scans the datastores according to the options that you selected.

After you finish

Check the alignment status of the virtual machines after VSC finishes scanning them.

Checking the alignment status of virtual machines

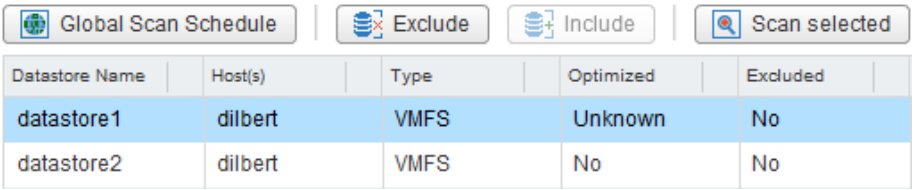
Check the alignment status of a virtual machine to determine whether it is aligned or misaligned. You should fix the alignment of a misaligned virtual machine to optimize I/O performance.

Before you begin

You should have scanned your datastores.

Steps

1. In the **Optimization and Migration** page, select a datastore from the datastores table (the table at the top of the page).



   After you select a datastore, the virtual machines running on that datastore appear in the virtual machines table (the table at the bottom of the Optimization and Migration page).

2. In the virtual machines table, view the **Alignment State** column to identify the alignment state of the virtual machines on that datastore.

   Tip: To quickly identify any misaligned virtual machines, select **Show only misaligned virtual machines**.

   Note: The View Disk Details button shows you the alignment details of a virtual machine's VMDKs.

   The following states can appear in the Alignment State column:

For this state...	Do this...
Actually aligned	Nothing. The partitions of the virtual machine's hard disk are aligned to the storage system and start at the correct offset.
Functionally aligned	Nothing. The partitions of the virtual machine's hard disk are misaligned; however, when residing on an optimized datastore, they align on correct boundaries. As a result, the virtual machine performs as though it is aligned. If you want to clone a functionally aligned virtual machine, you should take it offline and fix the VMDK alignment before you clone it. Otherwise, the clones can be misaligned if the destination datastores are not optimized for the VMDK layout of the clones.

For this state...	Do this...
Misaligned, Offline alignment only	Power down the virtual machine and align the VMDK using a tool such as VMware vCenter Converter. The virtual machine is misaligned; however, VSC cannot align it due to either of the following: • The virtual machine has more than one disk with different offsets • The virtual machine has multiple disks spanning multiple datastores
Misaligned, Online migration capable	Use VSC to perform an online alignment.
Other	Review the following reasons why VSC cannot determine the alignment state of the virtual machine: • It is inaccessible or reports an error during read attempts • It has a disk size of 0 • It does not have any partitions • It has independent disks or dynamic disks

3. Repeat steps 1 and 2 for each datastore.

Aligning the I/O of misaligned virtual machines non-disruptively

A misaligned virtual machine can negatively affect I/O performance. To correct the misalignment, Virtual Storage Console for VMware vSphere can migrate a virtual machine to a new or existing optimized datastore so that the I/O is functionally aligned. This process does not require downtime.

Before you begin

- You should have scanned your datastores and found virtual machines with the alignment state "Misaligned, Online migration capable."
- For NFS datastores, the storage system must be running Data ONTAP 8.1.3 or later.
- The volume on which the datastore resides must not be a SnapLock volume.
- You should be aware of the following caveats and limitations with optimized datastores:
  - You cannot use the vStorage APIs for Array Integration (VAAI) extended copy feature with an optimized datastore.
  - For NFS-optimized datastores, using Data ONTAP to perform an NDMP copy, NDMP restore, or dump restore to the volume can be slower.

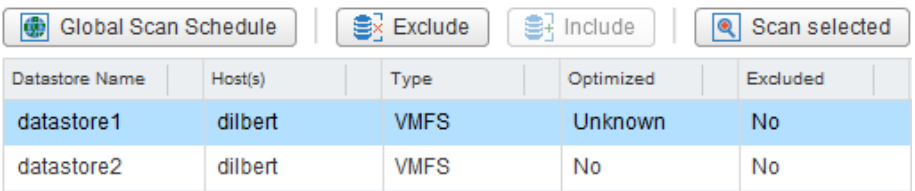
- Migrating a virtual machine from an optimized datastore to a non-optimized datastore will result in misaligned I/O to the virtual machine.

About this task

- Migrating multiple virtual machines at one time is I/O intensive.
  You should limit the number of virtual machines that you migrate at one time to avoid over-stressing your system.
- The alignment might require more space because deduplication is temporarily turned off when VSC aligns the virtual machine.

Steps

1. In the **Optimization and Migration** page, select a datastore on which a misaligned virtual machine is running.



   After you select a datastore, the virtual machines that reside on that datastore appear in the virtual machines table (the table at the bottom of the Optimization and Migration page).

2. In the virtual machines table, select one or more virtual machines with the status "Misaligned, Online migration capable."

   If you select multiple virtual machines, they must have the same offset group (the offset of the largest disk partition).

   You should limit the number of virtual machines that you migrate at one time to avoid over-stressing your system.

3. Click **Migrate**.

4. Complete the pages in the **Migrate Virtual Machines** wizard to migrate the virtual machine to an optimized datastore.

   a. In the **Destination datastore** page, specify whether you want to use an existing datastore or a new datastore.

      For existing datastores, you will be able to choose from datastores that are optimized for the offset group of the virtual machine.

b. (New datastore) In the **Name and type** page, specify a datastore name, datastore type (NFS or VMFS), and for a VMFS datastore, the VMFS protocol (FC/FCoE or iSCSI).
c. In the **Storage system** page, specify the storage system that you want to use for the datastore.
d. (Existing datastore) In the **Datastore selection** page, select the destination datastore.

   VSC lists the datastores that are optimized for the VMDK layout of the virtual machine. If no datastores are listed, go back and select the new datastore option.
e. (New datastore) In the **New datastore details** page, specify details about the datastore that you want to create.

   Most of the fields on this page are self-explanatory. The following table describes fields for which you might need guidance:

Field	Description
Thin provision	Allocates space on the volume when data is written, which allows you to provision more storage than is currently available. If disabled, space is reserved immediately. You must closely monitor the available space in the containing aggregate because thin provisioning can oversubscribe the available space. In an NFS configuration, you can enable auto grow to automatically expand the datastore when space is needed. Make sure that the value you specify for auto grow is larger than the size of the datastore.
Aggregate	Defines the aggregate on which you want to create a new volume. If you selected an SVM that is directly connected to VSC, striped aggregates appear as available; however, they are not supported. Provisioning to a striped aggregate will fail.
Volume	Specifies the volume on which you want to create the datastore. For clustered Data ONTAP, you should not create a datastore in the Storage Virtual Machine (SVM) root volume.
Auto grow	(NFS only) Automatically expands the datastore by the specified increment when space is needed, up to the size limit. This size limit you specify must be larger than the existing datastore.
Datastore cluster	Adds the datastore to a cluster if the Storage Distributed Resource Scheduler (SDRS) feature is enabled on the vCenter Server. Do not mix datastores with varying offsets in the same cluster and do not mix optimized and non-optimized datastores.

f. In the **Ready to complete** page, Review the summary of your selections and click **Finish**.

Result

VSC starts the migration task. You cannot cancel this task.

After you finish

If the old datastore is empty, use it for other virtual machines or destroy it.

Maintaining your VMware environment

You can use Virtual Storage Console for VMware vSphere to maintain your VMware environment by migrating virtual machines, redeploying virtual machines, reclaiming space from virtual machines, and managing datastores by mounting, resizing, and destroying them.

Migrating virtual machines to a new or existing datastore

Migrating virtual machines moves them from one datastore to another. For example, you might need to migrate a virtual machine to a new datastore to balance disk space usage.

Before you begin

- For NFS datastores, the storage system must be running Data ONTAP 8.1.3 or later.
- The volume on which the datastore resides must not be a SnapLock volume.
- To avoid migration errors, the virtual machines must be part of datastores that have been scanned by Virtual Storage Console for VMware vSphere.

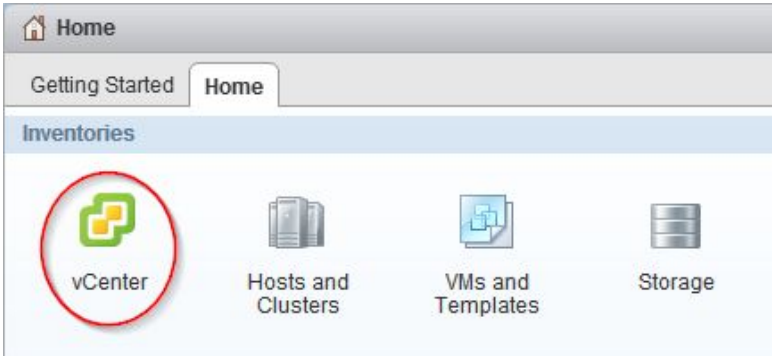
  Note: The Optimization and Migration page lists the offset group of a virtual machine, if its containing datastore was scanned.

About this task

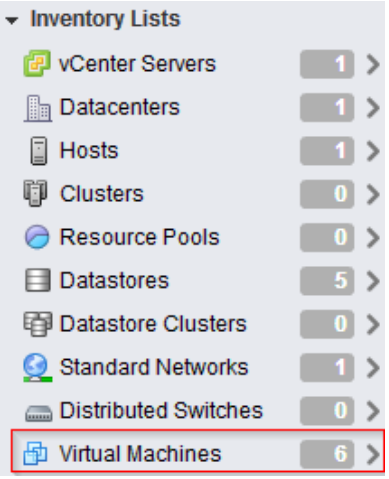
If the selected virtual machines do not have the same offset group, the target datastore will not be optimized for all virtual machines. VSC creates a datastore optimized for the offset group of the last virtual machine that it migrates.

Steps

1. From the vSphere Web Client **Home** page, click **vCenter**.



2. In the navigation pane, under **Inventory Lists**, click **Virtual Machines**.



3. In the **Objects** table, select the virtual machines that you want to migrate.

   Migrating multiple virtual machines at one time is I/O intensive. You should limit the number of virtual machines that VSC migrates at one time to avoid over-stressing your system.

4. Click **Actions > NetApp VSC > Migrate**.

5. Click **Yes** to confirm the action.

6. Complete the pages in the **Migrate Virtual Machines** wizard to migrate the virtual machines to a new or existing datastore.

   a. In the **Destination datastore** page, specify whether you want to migrate the virtual machines to an existing datastore or a new datastore.
   b. (New datastore) In the **Name and type** page, specify a datastore name, datastore type (NFS or VMFS), and for a VMFS datastore, the VMFS protocol (FC/FCoE or iSCSI).
   c. In the **Storage system** page, specify the storage system that you want to use for the datastore.
   d. (Existing datastore) In the **Datastore selection** page, select the destination datastore.
   e. (New datastore) In the **New datastore details** page, specify details about the datastore that you want to create.

      Most of the fields on this page are self-explanatory. The following table describes fields for which you might need guidance:

Field	Description
Thin provision	Allocates space on the volume when data is written, which allows you to provision more storage than is currently available. If disabled, space is reserved immediately. You must closely monitor the available space in the containing aggregate because thin provisioning can oversubscribe the available space. In an NFS configuration, you can enable auto grow to automatically expand the datastore when space is needed. Make sure that the value you specify for auto grow is larger than the size of the datastore.
Aggregate	Defines the aggregate on which you want to create a new volume. If you selected an SVM that is directly connected to VSC, striped aggregates appear as available; however, they are not supported. Provisioning to a striped aggregate will fail.
Volume	Specifies the volume on which you want to create the datastore. For clustered Data ONTAP, you should not create a datastore in the Storage Virtual Machine (SVM) root volume.
Auto grow	(NFS only) Automatically expands the datastore by the specified increment when space is needed, up to the size limit. This size limit you specify must be larger than the existing datastore.
Datastore cluster	Adds the datastore to a cluster if the Storage Distributed Resource Scheduler (SDRS) feature is enabled on the vCenter Server. Do not mix datastores with varying offsets in the same cluster and do not mix optimized and non-optimized datastores.

f. In the **Ready to complete** page, Review the summary of your selections and click **Finish**.

Result

VSC starts the migration task. You cannot cancel this task.

After you finish

If the old datastore is empty, use it for other virtual machines or destroy it.

Related concepts

Methods for migrating virtual machines on page 17

Redeploying NFS-based virtual machine clones from a template

After you clone virtual machines from a template, you might need to patch or update the cloned virtual machines. You can use Virtual Storage Console for VMware vSphere to redeploy NFS-based virtual machine clones from an updated template. Redeploying VMFS-based clones is not supported.

Before you begin

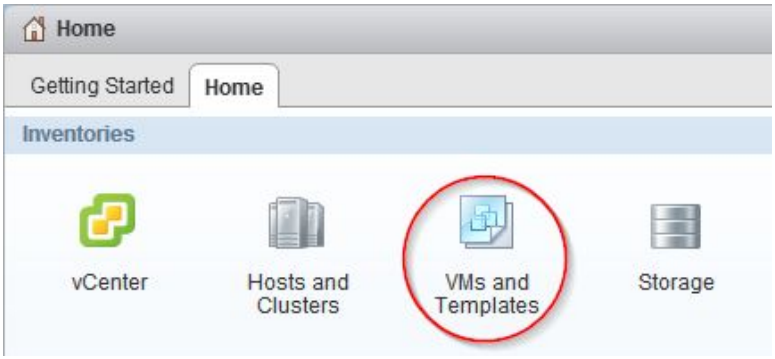
- You must have used VSC when you originally cloned the virtual machines from the template.
- Because redeploying resets the clone to the state of the template, you should first have backed up any needed data.

About this task

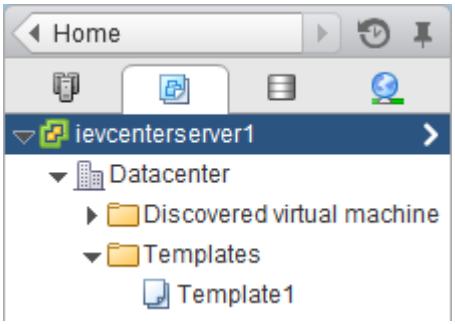
To redeploy a cloned virtual machine, VSC powers off the virtual machine. Make sure this is an acceptable time to take the virtual machine offline. VSC can power on the virtual machine after the redeployment is complete, if you select that option.

Steps

1. From the vSphere Web Client **Home** page, click **VMs and Templates**.



2. In the navigation pane, expand the datacenter that contains the virtual machine template.



3. Right-click the virtual machine and select **NetApp VSC > Redeploy Clones**.
4. In the **Redeploy Clones** dialog box, select the clones, choose their settings, and click **OK**.

   The clones can inherit the VMware specification and power state from the template, or you can define new settings.

   For a large number of virtual machines, stagger the start up of those virtual machines so you do not overwhelm your system.

   Note: If a problem prevents VSC from starting some of the virtual machines, the delay could result in VSC powering on a large number of virtual machines at once. For example, if you specify 10 virtual machines per minute and the start is delayed by five minutes, VSC starts 50 virtual machines at once. After the delay, VSC starts the specified number of virtual machines per minute.
5. To confirm that you want to power off and redeploy the selected virtual machines, click **OK**.

Result

VSC powers off the virtual machines and redeploys them based on the new template. After the redeployment, VSC powers on the virtual machines, if you chose that option.

Related tasks

Cloning virtual machines from a template on page 116

Reclaiming space from NFS-based virtual machines

When users delete data from a virtual machine, the storage space from NTFS partitions is not immediately returned to the NFS datastore. You can reclaim the space to return it to the datastore. Reclaiming space from VMFS-based virtual machines is not supported.

Before you begin

- Virtual machine files must be on NFS datastores that are not backed by a qtree on a vFiler unit.
- VMDKs must have NTFS partitions.
- VMware Tools must be installed on the virtual machine.

- ISOs mounted to the virtual machine must be contained in an NFS datastore.

About this task

To reclaim the space, VSC powers off a virtual machine by using VMware Tools. Make sure this is an acceptable time to take the virtual machine offline. After the process completes, VSC returns the virtual machine to its previous state.

You can perform this task on an individual virtual machine or on a datastore, which reclaims space from all virtual machine disks in a datastore. If you do not want to take all of the virtual machines in a datastore offline, reclaim the space from one virtual machine at a time.

Steps

1. Reclaim space from one or more virtual machines:

To...	Do the following...
Reclaim space from all virtual machines in a datastore	From the vSphere Web Client Home page, click **Storage**.
Reclaim space from one virtual machine	From the vSphere Web Client Home page, click **VMs and Templates**.

2. In the navigation pane, expand the datacenter that contains the datastore or the virtual machine.
3. Right-click the datastore or virtual machine and select **NetApp VSC > Reclaim Space**.
4. In the **Reclaim Space** dialog box, click **OK**.

Result

VSC powers off the virtual machines and starts reclaiming the space.

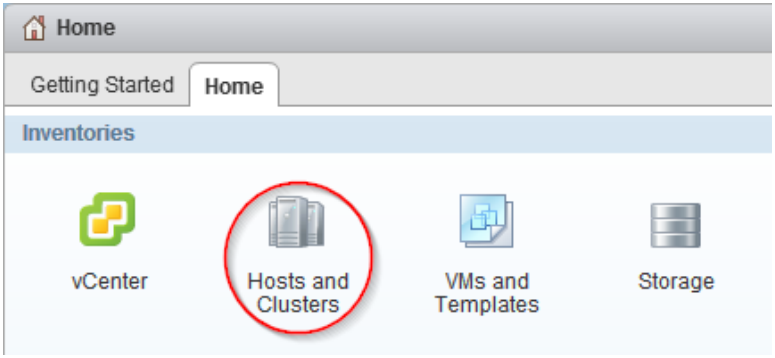
Do not power on the virtual machines while space reclamation is in progress.

Mounting datastores on hosts

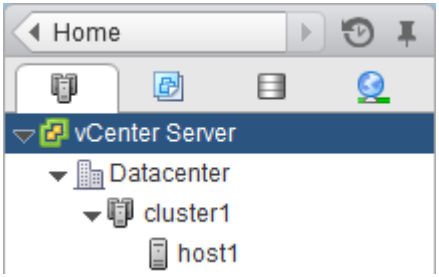
Mounting a datastore gives a host access to storage. You might need to mount a datastore on a host after you add the host to your VMware environment.

Steps

1. From the vSphere Web Client **Home** page, click **Hosts and Clusters**.



2. In the navigation pane, expand the datacenter that contains the host.



3. Right-click the host and select **NetApp VSC > Mount Datastores**.
4. Select the datastores that you want to mount and click **OK**.

Result

VSC mounts the datastores on the host.

Resizing datastores

Resizing a datastore gives you more or less storage for your virtual machine files. You might need to change the size of a datastore as your infrastructure requirements change.

Before you begin

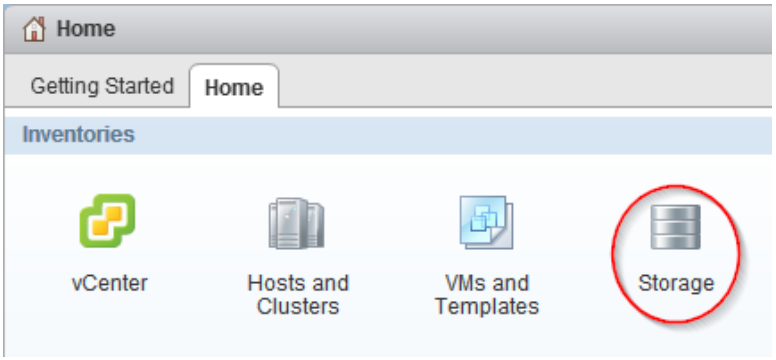
If you want VSC to resize the containing volume when it resizes the VMFS datastore, you should have enabled the **Create new volume for each new LUN** option in the VSC provisioning options for the storage system.

About this task

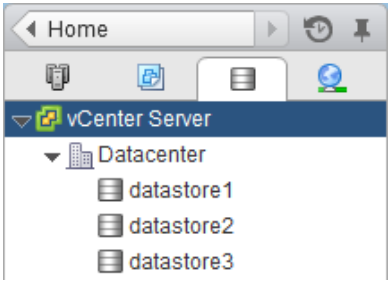
You can increase or decrease the size of an NFS datastore. You can only increase the size of a VMFS datastore.

Steps

1. From the vSphere Web Client **Home** page, click **Storage**.



2. In the navigation pane, expand the datacenter that contains the datastore.



3. Right-click the datastore and select **NetApp VSC > Resize**.
4. In the **Resize** dialog box, specify a new size for the datastore and click **OK**.

Result

VSC resizes the datastore.

Related tasks

Managing settings for volumes on page 107

Destroying datastores

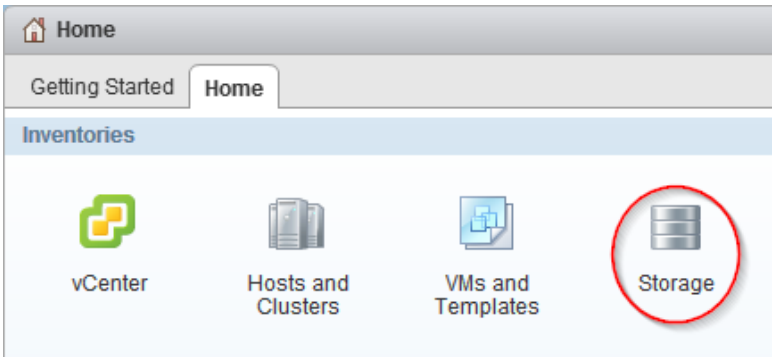
Destroying a datastore returns storage to your storage system and deletes associated objects such as export policies and igroups. You might need to destroy a datastore when you decommission your virtual machines.

About this task

When you destroy a datastore, the virtual machines within that datastore are also destroyed. Virtual Storage Console for VMware vSphere displays a list of the affected virtual machines before you destroy the datastore.

Steps

1. From the vSphere Web Client **Home** page, click **Storage**.



2. In the navigator pane, right-click the datastore and select **NetApp VSC** > **Destroy**.
3. Click **OK**.

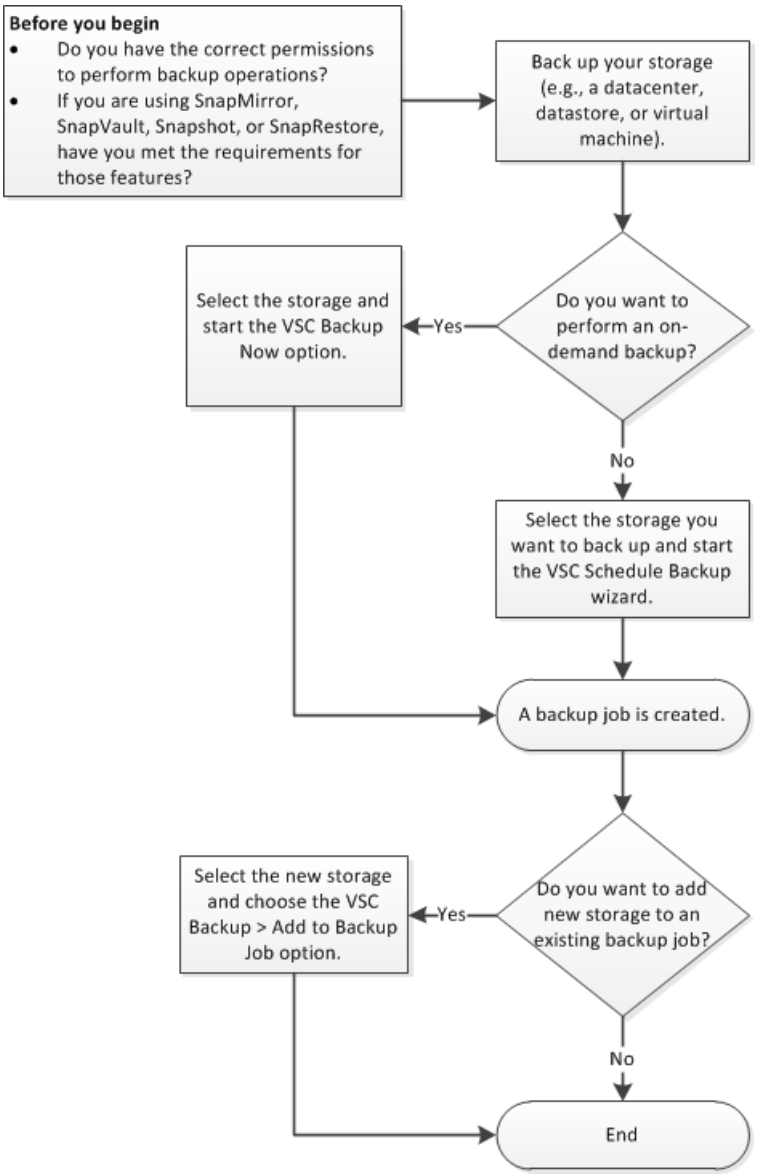
Result

VSC destroys the datastore.

Backing up virtual machines and datastores

You can back up individual virtual machines or datastores on demand or on an automated schedule using Virtual Storage Console for VMware vSphere.

You can set a backup job schedule and specify a retention policy for the backup copy when you create a new backup job using the backup wizard. You can also change the schedule and retention policy, as well as suspend and resume or delete a backup job.



Related concepts

Creating custom user accounts for backup and restore operations on page 203
VSC CLI commands on page 205

Related tasks

Performing an on-demand backup of a virtual machine or datastore on page 141

Scheduling backup jobs on page 143
Adding a virtual machine or datastore to an existing backup job on page 145

Backup job specifications

Before you create a backup job, you should be aware of the information that you can specify to ensure that the backup schedule, the backup retention policy, and the alert notifications of backup activity for your job perform as expected.

When you add a new backup job, you can specify whether you want to initiate a SnapMirror or SnapVault update on the virtual entities that are to be backed up or create VMware snapshots for every backup. If you select virtual machines that span multiple datastores, you can specify one or more of the datastores to be excluded from the backup.

If you want to run a backup script that is installed on the server with this job, you can choose the scripts that you want to use. If you create a prebackup or postbackup script that results in an output file when the script is run, the output file is saved to the same directory to which you initially installed the prebackup or postbackup script. You can specify the hourly, daily, weekly, or monthly schedule that you want applied to your backup job, or you can add a backup job without attaching a schedule to the backup.

You can specify the maximum number of days or the maximum number of backup copies and email alerts for this backup job. You must first set the SMTP server and the destination email addresses to receive an alert notification when an alarm is triggered or the system status changes. You can enable or disable alarms and specify how often you receive email alerts when an error or warning occurs. The **Notify on** options in the Schedule Backup wizard include the following:

Always	An alert notification is always sent.
Errors or Warnings	A backup failure or a warning triggers an alert notification.
Errors	A backup failure or partial failure triggers an alert notification.
Never	An alert notification is never sent.

Backup job requirements

A SnapRestore license is required to perform restore operations and a SnapMirror and SnapVault license is required if you are going to use the SnapMirror or SnapVault options for a backup job.

The following is a SnapRestore requirement:

- SnapRestore technology must be licensed for the storage systems where the datastore and virtual machine system images reside.

Following are some SnapMirror and SnapVault requirements:

- The volumes containing the active datastore and virtual machine images must be configured as SnapMirror or SnapVault source volumes.
- The SnapVault policy must have a rule that specifies labels for the VSC backup schedule:

Schedule type	Required label
Hourly	VSC_JOB_HOURLY
Daily	VSC_JOB_DAILY
Weekly	VSC_JOB_WEEKLY
Monthly	VSC_JOB_MONTHLY
One-time only	VSC_ONDEMAND

  To use values other than the default values, you must specify the following labels in the `smvi.config` file and specify the same labels when you create the SnapVault protection policy.

  ```
  "snapvault.job.hourly.label"="VSC_XXXX"
  "snapvault.job.daily.label"="VSC_XXXX"
  "snapvault.job.weekly.label"="VSC_XXXX"
  "snapvault.job.monthly.label"="VSC_XXXX"
  "snapvault.ondemand.label"="VSC_XXXX"
  ```

- The source volumes must have a SnapMirror or SnapVault relationship with target volumes on a second storage system that is licensed for SnapMirror or SnapVault.
- The host names and IP addresses of the SnapMirror or SnapVault source and destination storage systems must be resolvable for the SnapManager for Virtual Infrastructure server, either through a configured DNS server or through host entries added to the host file on the SnapManager for Virtual Infrastructure server.
- Cluster or Storage Virtual Machine (SVM) administrators must create node-management or cluster-management LIFs, which are required to update SnapMirror or SnapVault relationships for storage systems running clustered Data ONTAP 8.2 or later. The cluster-management LIF is required for storage systems running a version of clustered Data ONTAP prior to 8.1.

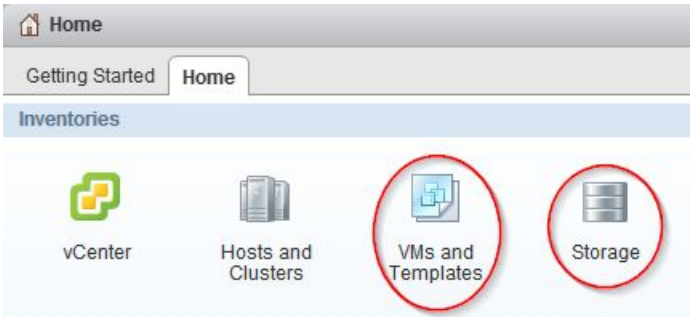
Performing an on-demand backup of a virtual machine or datastore

You can launch a one-time backup operation for a virtual machine or for an entire datastore. This type of backup is useful if you do not want to schedule regular backups for a particular virtual

machine or selected datastores or if you need to create a one time, non-scheduled backup to retain important changes.

Steps

1. From the vSphere Web Client **Home** page, click **VMs and Templates** to view virtual machines or click **Storage** to view datastores.



2. In the navigation pane, expand the datacenter that contains the virtual machine or datastore depending on whether you are in the **VMs and Templates** view or the **Storage** view.
3. Right-click the datastore or virtual machine and select **NetApp VSC > Backup > Backup Now**.
4. In the **Backup Now** dialog box, type a name for the backup job.
5. Optional: Check the box next to the options you want this backup job to use:
   - If you want to start a SnapVault update on the selected entities concurrent with every backup copy, select **Initiate SnapVault update**.

     Note: The SnapVault option is only supported on clustered Data ONTAP 8.2 or later.

     For this option to execute successfully, the selected entities must reside in volumes that are configured as SnapVault source volumes and a destination volume must also exist.
   - If you want to start a SnapMirror update on the selected entities concurrent with every backup copy, select **Initiate SnapMirror update**.

     For this option to execute successfully, the selected entities must reside in volumes that are configured as SnapMirror source volumes and a destination volume must also exist.

     The SnapManager for Virtual Infrastructure server should be able to resolve the host name and IP address of the source and destination storage systems in the `snapmirror.conf` file.
   - If you want to create a VMware snapshot every time the backup job runs, select **Perform VMware consistency snapshot**.
   - If you want to include independent disks from datastores that contain temporary data, select **Include datastores with independent disks**.
6. Click **OK**.

Scheduling backup jobs

You can create scheduled backup jobs by selecting an entire datacenter, a datastore, or a virtual machine. You can also view all backup jobs on the Backup Jobs page in the vSphere Web Client and create backup jobs from this page using the backup job wizard to select a virtual entity.

Before you begin

The vSphere Web Client must be connected to a vCenter Server to create backup copies.

About this task

You can set the schedule for your backup jobs, specify a retention policy, and create an automated policy for email alerts.

Steps

1. To create and schedule a backup job, take one of the following actions:

To...	Do this...
Create a backup job for a specific datastore or virtual machine	**a.** From the vSphere Web Client Home page, click **VMs and Templates** to view virtual machines or click **Storage** to view datastores. **b.** In the navigation pane, expand the datacenter that contains the virtual machine or datastore depending on whether you are in the **VMs and Templates** view or the **Storage** view. **c.** Right-click the datastore or virtual machine and select **NetApp VSC > Backup > Schedule Backup**. You can create a scheduled backup job for an entire datacenter by right-clicking the datacenter and selecting **NetApp > Backup > Schedule Backup**.
Create a backup job using the backup job wizard to select a datastore or virtual machine	**a.** From the vSphere Web Client Home page, click **vCenter**. **b.** In the navigation pane, under NetApp, click **Backup Jobs**. **c.** Click the Add icon on the Backup Jobs page in the vSphere Web Client.

2. Type a name for the backup job and add a description.
3. Optional: Check the box next to the options you want for this backup job:
   - If you want to start a SnapVault update on the selected entities concurrent with every backup copy, select **Initiate SnapVault update**.

     Note: The SnapVault option is only supported on clustered Data ONTAP 8.2 or later.

For this option to execute successfully, the selected entities must reside in volumes that are configured as SnapVault source volumes and a destination volume must also exist.

- If you want to start a SnapMirror update on the selected entities concurrent with every backup copy, select **Initiate SnapMirror update**.
  For this option to execute successfully, the selected entities must reside in volumes that are configured as SnapMirror source volumes and a destination volume must also exist.
  The SnapManager for Virtual Infrastructure server should be able to resolve the host name and IP address of the source and destination storage systems in the `snapmirror.conf` file.
- If you want to create a VMware snapshot every time the backup job runs, select **Perform VMware consistency snapshot**.
- If you want to include independent disks from datastores that contain temporary data, select **Include datastores with independent disks**.

4. Click **Next**.
5. If you have not selected a datastore or virtual machine, select the virtual entities available for this backup job and click **Next**.
6. Select the spanned entities available for this backup job and click **Next**.

   Spanned entities might be a VM with multiple VMDK's across multiple datastores.
7. Select one or more backup scripts and click **Next**.

   If an error message appears, indicating that at least one of the selected scripts has been deleted, you can save the backup job without any script in the selected scripts list, thereby removing the deleted script from the job. Otherwise, the backup job continues to use the deleted script.
8. Select the hourly, daily, weekly, or monthly schedule that you want for this backup job.
9. Specify either a maximum number of days, or maximum number of backup copies for this backup job and click **Next**.

   Attention: If you select **A Maximum of Backups**, you can specify a number up to 254; you cannot specify the maximum of 255 backup copies per backup job.
10. Select **Use default vCenter credentials** or type the user name and password for a specific vCenter Server user.
11. Select the frequency for receiving email alerts and click **Next**.

    You can add multiple email addresses by using semicolons to separate each email address.
12. Optional: Click **Send Test Email** to verify that the outgoing email server where the alert notifications are to be sent is working correctly.
13. Review the summary of your selections and click **Finish**.
14. Optional: Select the **Run Job Now** check box to immediately run the job.

Related tasks

Modifying the job properties of a scheduled backup job on page 146

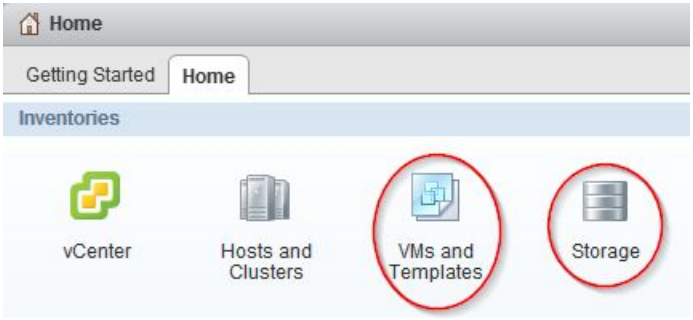
Suspending an active backup job on page 146
Resuming a suspended backup job on page 147
Deleting a scheduled backup job on page 148

Adding a virtual machine or datastore to an existing backup job

You can add a new virtual machine or datastore to an existing backup job. If you have already created a backup job with specific schedule and retention properties, you can then add a new datastore or virtual machine to the existing backup job.

Steps

1. From the vSphere Web Client **Home** page, click **VMs and Templates** to view virtual machines or click **Storage** to view datastores.



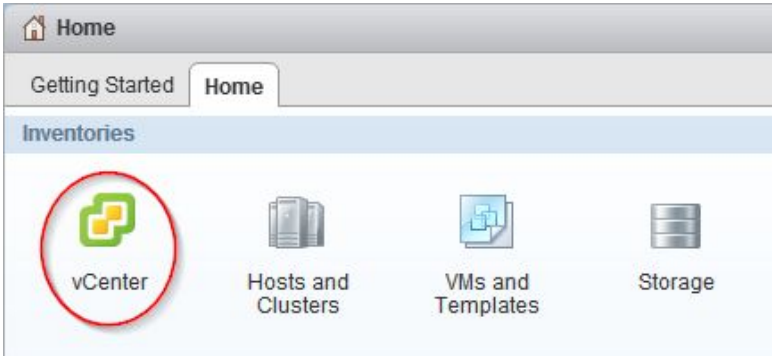
2. In the navigation pane, expand the datacenter that contains the virtual machine or datastore depending on whether you are in the **VMs and Templates** view or the **Storage** view.
3. Right-click the datastore or virtual machine and select **NetApp VSC > Backup > Add to Backup Job**.
4. In the **Add to Backup Job** dialog box, select the backup job to which you want to add the datastore or virtual machine.
5. Click **OK**.

Modifying the job properties of a scheduled backup job

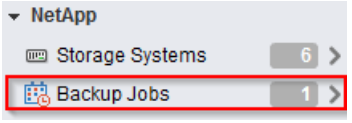
You can modify the name and description, the datastores and virtual machines that are assigned, the backup scripts, the user credentials, the schedule, the retention policy, and the email alerts for an existing backup job using the Modify Backup Job dialog box.

Steps

1. From the vSphere Web Client **Home** page, click **vCenter**.



2. In the navigation pane, under **NetApp**, click **Backup Jobs**.



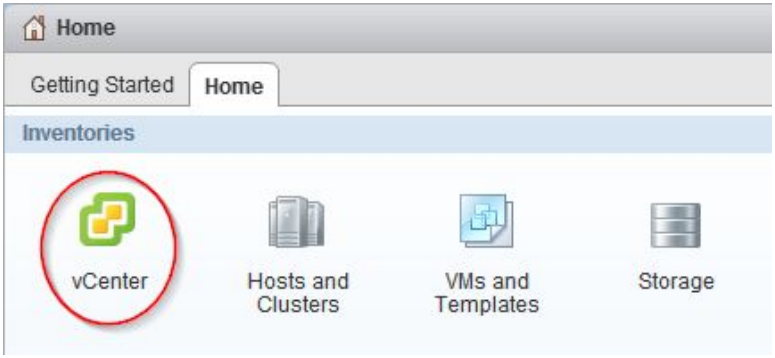
3. Right-click the backup job whose properties you want to modify and select **Modify**.
4. Click the appropriate tab for the properties that you want to modify for this backup job.
5. Modify backup job properties as necessary, and then click **OK** to change the properties.

Suspending an active backup job

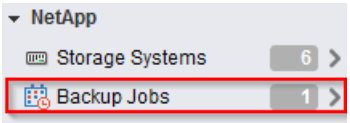
You can suspend the scheduled operations of an active backup job without deleting the job. This gives you the ability to temporarily halt backup jobs in case of planned maintenance, during periods of high activity, or for other reasons.

Steps

1. From the vSphere Web Client **Home** page, click **vCenter**.



2. In the navigation pane, under **NetApp**, click **Backup Jobs**.



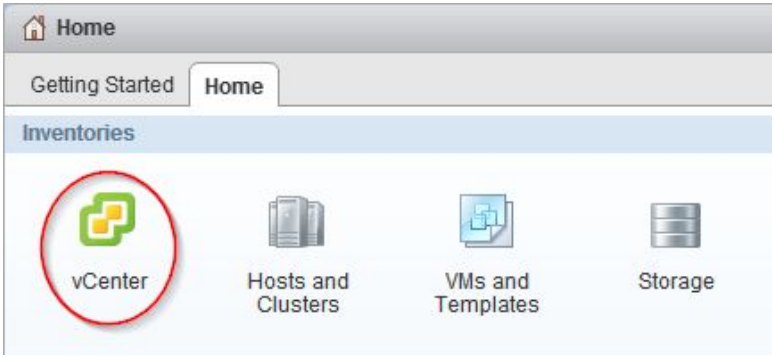
3. Right-click the active backup job that you want to suspend and select **Suspend**.
4. Click **OK** when you receive the confirmation prompt to suspend the active backup job.

Resuming a suspended backup job

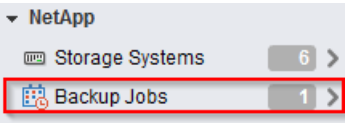
You can resume and run a suspended backup job at any time after you temporarily halt the backup job.

Steps

1. From the vSphere Web Client **Home** page, click **vCenter**.



2. In the navigation pane, under **NetApp**, click **Backup Jobs**.



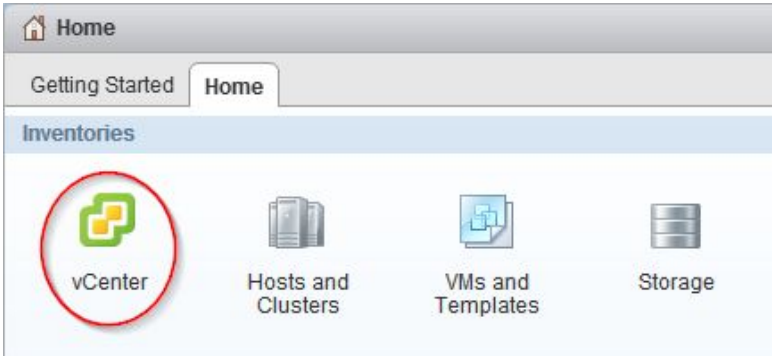
3. Right-click the suspended backup job that you want to resume and select **Resume**.
4. Click **OK** when you receive the confirmation prompt to resume the suspended backup job.

Deleting a scheduled backup job

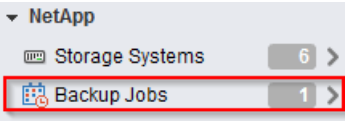
You can select and delete one or more backup jobs from the list of scheduled jobs, but you cannot delete any backup jobs that are running.

Steps

1. From the vSphere Web Client **Home** page, click **vCenter**.



2. In the navigation pane, under **NetApp**, click **Backup Jobs**.



3. Select one or more backup jobs that you want to delete.
4. Right-click each selected backup job, and then select **Delete**.
5. Click **OK** at the confirmation prompt to delete the scheduled backup job.

Restoring virtual machines and datastores from backup copies

You can restore your virtual machines and datastores from backup copies using Virtual Storage Console for VMware vSphere. Virtual machines are always restored to the most current datastore; only VMDKs can be restored to an alternate datastore.

Related concepts

Creating custom user accounts for backup and restore operations on page 203
VSC CLI commands on page 205

Related tasks

Restoring data from backup copies on page 152
Mounting a backup copy on page 150
Unmounting a backup copy on page 151

Considerations for restore operations using data that was backed up with failed VMware consistency snapshots

Even if a VMware consistency snapshot for a virtual machine fails, the virtual machine is nevertheless backed up. You can view the backed up entities contained in the backup copy in the Restore wizard and use it for restore operations.

When creating a VMware snapshot, the virtual machine pauses all running processes on the guest operating system so that file system contents are in a known consistent state when the Data ONTAP Snapshot copy is taken. Despite the VMware snapshot failure, the virtual machine is still included in the Data ONTAP Snapshot copy.

The Quiesced column can display the following values:

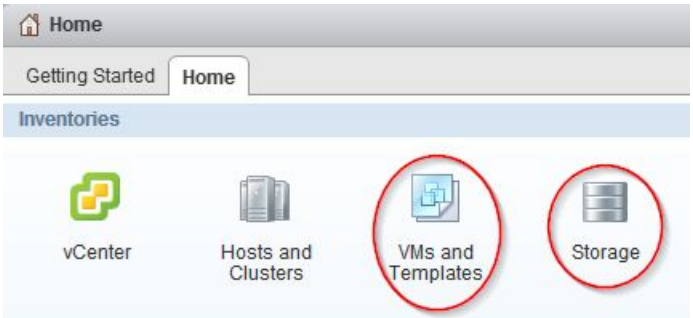
- Yes, if a VMware snapshot operation was successful and the guest operating system was quiesced.
- No, if a VMware snapshot was not selected or the operation failed because the guest operating system could not be quiesced.
- Not Applicable, for entities that are not virtual machines.

Searching for backup copies

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

Steps

1. From the vSphere Web Client **Home** page, click **VMs and Templates** to view virtual machines or click **Storage** to view datastores.



2. In the navigation pane, expand the datacenter that contains the virtual machine or datastore, depending on whether you are in the **VMs and Templates** view or the **Storage** view.
3. Right-click the datastore or virtual machine and select **NetApp VSC > Restore**.
4. Click **Advanced Filter** in the **Restore** wizard.
5. Type one or more search terms, and then click **OK**.

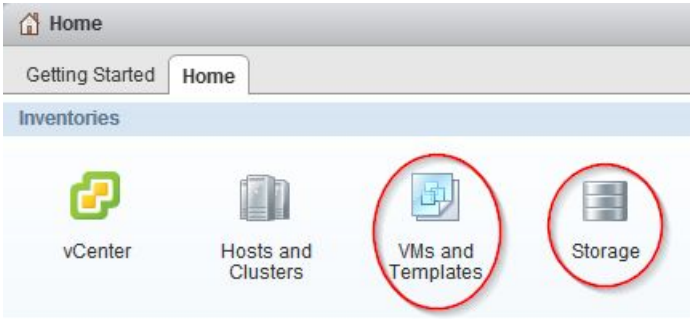
   Available criteria for search are the name of the backup job, time range of the backup job, whether the backup job contains a VMware snapshot, or whether the backup job has been mounted.

Mounting a backup copy

You can mount an existing backup copy onto an ESX server to verify the contents of the backup copy prior to completing a restore operation.

Steps

1. From the vSphere Web Client **Home** page, click **VMs and Templates** to view virtual machines or click **Storage** to view datastores.



2. In the navigation pane, expand the datacenter that contains the virtual machine or datastore depending on whether you are in the **VMs and Templates** view or the **Storage** view.
3. Right-click the datastore or virtual machine and select **NetApp VSC > Backup > Mount Backup**.
4. In the **Mount Backup** dialog box, select the name of an unmounted backup copy that you want to mount.
5. Select the name of the ESX server to which you want to mount the backup copy.

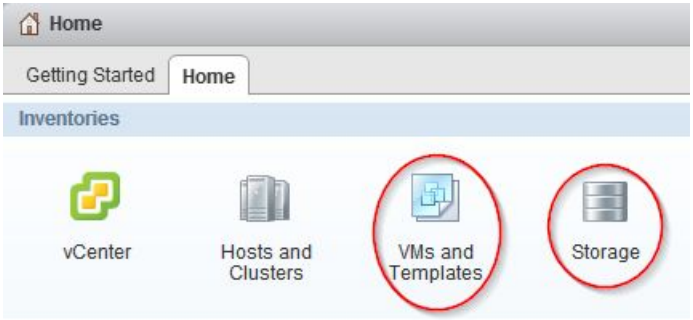
   You can only mount one backup copy at a time, and you cannot mount a backup that is already mounted. All datastores residing in the backup copy, even ones that were added because of spanned VMs, are mounted.
6. Click **OK**.

Unmounting a backup copy

After you have verified the contents of a mounted backup copy, you can unmount it from the ESX server. When you unmount a backup, all of the datastores in that backup copy are unmounted and are no longer visible from the ESX server.

Steps

1. From the vSphere Web Client **Home** page, click **VMs and Templates** to view virtual machines or click **Storage** to view datastores.



2. In the navigation pane, expand the datacenter that contains the virtual machine or datastore depending on whether you are in the **VMs and Templates** view or the **Storage** view.
3. Right-click the datastore or virtual machine and select **NetApp VSC > Backup > Unmount Backup**.
4. In the **Unmount Backup** dialog box, select the name of a mounted backup that you want to unmount.
5. Click **OK**.

Restoring data from backup copies

You can restore a datastore, an entire virtual machine or particular virtual disks of a given virtual machine. By doing so, you overwrite the existing content with the backup copy you select.

Before you begin

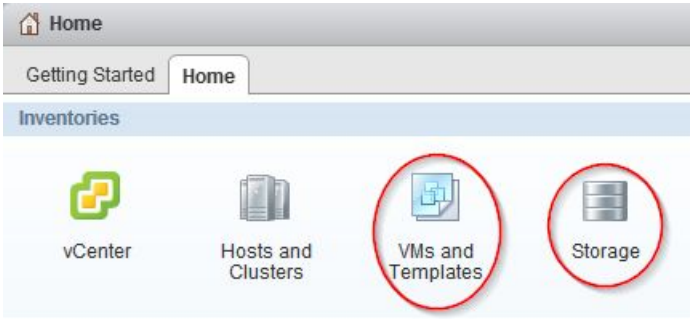
You must have already backed up a virtual machine before you can restore either the entire VM or its individual VMDKs.

About this task

If you are restoring a virtual machine to a second ESX server, the virtual machine is unregistered from the first ESX server and the restored virtual machine is placed on the second ESX server. Both ESX servers must share the same datastore.

Steps

1. From the vSphere Web Client **Home** page, click **VMs and Templates** to view virtual machines or click **Storage** to view datastores.



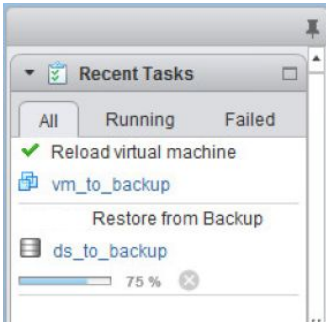
2. In the navigation pane, expand the datacenter that contains the virtual machine or datastore depending on whether you are in the **VMs and Templates** view or the **Storage** view.
3. Right-click the datastore or virtual machine and select **NetApp VSC > Restore**.
4. In the **Restore** wizard, select the backup copy that you want to restore from and click **Next**.

5. Select one of the following restore options:

Option	Description
The entire virtual machine	Restores the contents to the last datastore in which it resided from a Snapshot copy with a particular time and date. The **Restart VM** check box is enabled if you select this option and the virtual machine is registered.
Particular virtual disks	Restores the contents of individual VMDKs to the most current or alternate datastore. This option is enabled when you clear the **The entire virtual machine** option.

6. Click **Next**.
7. Review the summary of your selections and click **Finish**.

   You can track the progress of the restore operation from the Recent Tasks pane in the vSphere Web Client.



Troubleshooting

This section describes how to troubleshoot general VSC for VMware vSphere installation and usage issues.

Information at NetApp VSC Communities Forum

The NetApp Communities Forum provides information about Virtual Storage Console for VMware vSphere. When you join the forum you can ask questions and talk with other VSC users.

The NetApp Communities Forum also provides information about tools you can use with VSC news. At the forum, you can do the following:

- Get links to tools, such as the "RBAC User Creator for Data ONTAP."
- See video blogs created by NetApp VSC team members.
- See the latest NetApp news about VSC, such as when a beta testing program might be available.

It is good practice to check the NetApp Communities Forum periodically.

The NetApp VSC Communities Forum is online at:

http://communities.netapp.com/vsc

Check the Release Notes

The *Release Notes* contain the most up-to-date information about known problems and limitations. The *Release Notes* also contain information about how to look up information about known bugs.

The *Release Notes* are updated when there is new information about Virtual Storage Console for VMware vSphere. It is a good practice to check the *Release Notes* before you install VSC, and any time you encounter a problem with VSC.

You can access the *Release Notes* from the the NetApp Support Site at *support.netapp.com*.

Uninstall does not remove standard VSC roles

When you uninstall Virtual Storage Console for VMware vSphere, the standard VSC roles remain. This is expected behavior and does not affect the performance of VSC or your ability to upgrade to a new version of VSC. You can manually delete these roles, if you choose.

While the uninstall program does not remove the roles, it does remove the localized names for the VSC-specific privileges and append the following prefix to them: "XXX missing privilege". For example, if you open the vSphere Edit Role dialog box after you install VSC, you will see the VSC-

specific privileges listed as `XXX missing privilege.<privilege name>.label not found XXX`.

This behavior happens because the vCenter Server does not provide an option to remove privileges.

When you reinstall VSC or upgrade to a newer version of VSC, all the standard VSC roles and VSC-specific privileges are restored.

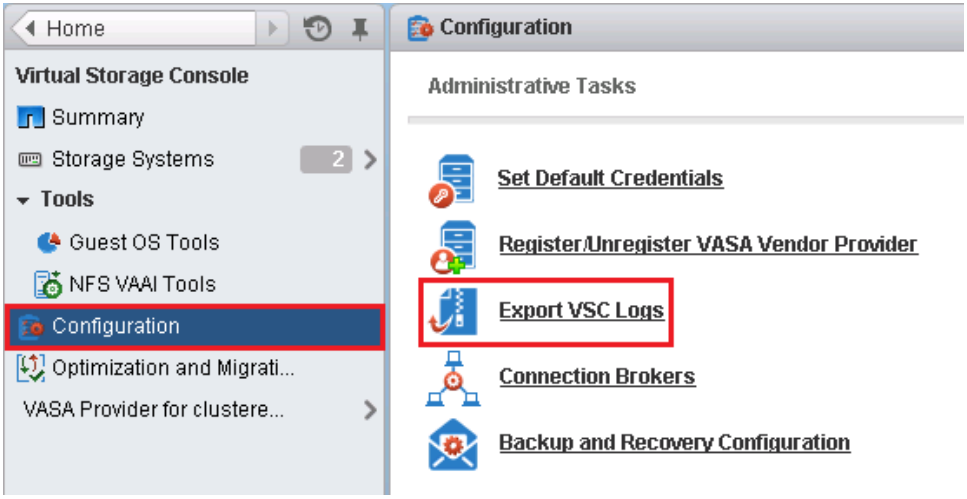
Collecting the VSC for VMware vSphere log files

You can collect the Virtual Storage Console for VMware vSphere log files using the Export VSC Logs page. Technical support might ask you to collect the log files to help troubleshoot a problem.

Steps

1. From the Virtual Storage Console **Home** page, click **Configuration > Export VSC Logs**.

   This operation can take several minutes.



2. When prompted, save the file to your local computer.

After you finish

Send the .zip file to technical support.

Updating vCenter credentials for background discovery

If the vCenter credentials specified when Virtual Storage Console for VMware vSphere was installed expire, Monitoring and Host Configuration can no longer run background discovery tasks.

Monitoring and Host Configuration then displays an error message. Re-register VSC to enter updated credentials.

Before you begin

The vCenter account must be an administrator-level account.

Steps

1. Click the link in the error message about expired credentials, or point a Web browser to the registration Web page:

   https://*hostname*:8143/Register.html

   hostname is the host name or IP address of the server where VSC is installed.

   If a security certificate warning is displayed, choose the option to ignore it or to continue to the Web site.

   The Plugin registration Web page is displayed with the current credentials.
2. Enter the new password for the user name shown, or enter a new user name and password.
3. Restart all vCenter Clients.

Resolution of issues that apply to backup and restore operations

If you encounter unexpected behavior during a backup or restore operation, you can follow specific troubleshooting procedures to identify and resolve the cause of such issues.

Values that you can override for backup jobs

To improve operational efficiency, you can modify the `smvi.override` configuration file to override the default values specified in the file. These values control such settings 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 `smvi.override` configuration file is located in the installation directory at `C:\Program Files\NetApp\VSC\smvi\server\etc\smvi.override`.

You can modify the following entries if you need to override the default values and if you modify any of these entries, you must restart the server for the changes to take effect.

`vmware.max.concurrent.snapshots=6`	Specifies six as the default maximum number of VMware snapshots created or deleted per datastore during a backup.

vmware.quiesce.retry.count=0	Specifies zero as the maximum number of retry attempts for VMware snapshots.
vmware.quiesce.retry.interval=5	Specifies the amount of time, in seconds, between retry attempts for VMware snapshots.
vim.client.log.verbose=true	When the value is true, logs the interactions between the SMVI server and the vCenter server.
smvi.script.timeout.seconds=120	Specifies the SMVI timeout value for a pre-backup or post-backup script, which is when the SMVI server stops waiting for the script to finish running.

Location of backup event and error logs

Virtual Storage Console logs both server messages and messages between the server and the user interface, including detailed information about event messages and errors. Reviewing these logs helps you troubleshoot any errors that occur during backup or restore operations.

The log files are stored under the installation directory at the following locations:

- The server log messages are at `C:\Program Files\NetApp\Virtual Storage Console\smvi\server\log\server.log`.
- The log messages between the user interface and the server are at `C:\Program Files\NetApp\Virtual Storage Console\log\smvi.log`.

Email notification for scheduled backup contains a broken link

Issue	When you click the link to view the log files in the email notification for a backup job, an error occurs.
Cause	This problem occurs if you disable the IP address of the network adapters for the SMVI log viewer.
Corrective action	You must enable the IP address of the network adapters for the SMVI log viewer in one of the following ways, depending on your operating system: • Select **Control Panel** > **Network connections** > **Network and Sharing Center** in Windows 2003, Windows 2008, Windows 2008 R2, and Windows 7 environments. • Select **Control Panel** > **Network connections** in Windows Vista and Windows XP environments.

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

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

Description	This message occurs when you attempt 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 and the mount operation fails.
Corrective action	When you add a storage system running clustered Data ONTAP to Virtual Storage Console, use the server IP address instead of the Storage Virtual Machine (SVM) IP address.

Error writing backup metadata to repository\backups.xml: move failed

Description	This message occurs when Backup and Recovery attempts to rename a temporary file during the process of creating of a new backups.xml file with updated backup information. The new file is saved to the Backup and Recovery repository folder.
Corrective action	You must disable any antivirus programs that are running a scan of the Backup and Recovery repository folder. For a typical Windows installation, the repository can be found at the following location: • `C:\Program Files\NetApp\Virtual Storage Console\smvi\server\repository`.

Virtual Storage Console unable to discover datastores on a Storage Virtual Machine (SVM) without a management LIF

Issue	Running a scheduled backup job fails.
Cause	This problem occurs when a Storage Virtual Machine (SVM) without a management LIF is added in Virtual Storage Console. VSC cannot resolve this Storage Virtual Machine (SVM) and is unable to discover any datastores or volumes on the Storage Virtual Machine (SVM) on which to perform backup or restore operations.
Corrective action	You must add a Storage Virtual Machine (SVM) with a management LIF before you can perform backup or restore operations.

VMware vSphere does not remove all snapshot delta disks during a restore operation

Issue	When you delete a VMware snapshot, the snapshot delta disks that are created after quiescing the virtual machine are not removed.
Cause	This problem occurs during a backup of a virtual machine running on Windows 2008 or Windows 2008 R2. Virtual Storage Console for VMware vSphere creates a quiesced VMware snapshot, which results in the creation of snapshot delta disks. When you successfully restore the VM in VSC and then revert to the snapshot

taken during the backup process and ultimately delete the VMware snapshot, not all the delta disk files are deleted.

Corrective action None

Provisioning and cloning programmable API

Virtual Storage Console for VMware vSphere supports a programmable application interface (API) for provisioning and cloning operations. The API is designed to be leveraged with the VI SDK. It provides end-to-end automated datastore provisioning and offloads the intricacies of storage object cloning while cloning virtual machines.

Note: The VSC provisioning and cloning operations perform the same role-based access control checks that VSC performs.

The managed object reference returned by the VMware VI SDK is used to identify components in the vCenter Inventory. You can view this information using the Managed Object Browser on the vCenter Server.

The API is exposed using Simple Object Access Protocol (SOAP). It provides a layer above the NetApp Manageability SDK and the VMware VI SDK, but it does not require these in the customer application or script.

This version of the API exposes the virtual machine clone creation engine (which includes the redeploy feature), the datastore management engine (create, destroy, resize), and the file copy/clone offload engine. There are also two general-purpose utility methods included:

- `getVmFiles` returns a list of files that make up the virtual machine. This is useful for creating the list of files required in the `cloneSpec` API.
- `getMoref` returns the managed object reference of the requested object based on name and type. The `getMoref` returns the first object that matches the name and type combination. For this reason, this method should not be used in production environments unless all object names are unique.

The virtual machine clone engine

The virtual machine clone engine provides two clone creation and routing methods: createClones and redeployVMs.

- `createClones` can be used to create virtual machine clones on new or existing datastores. When more than one datastore is created, the FlexClone feature on the controller is leveraged to create clones of the datastore.
- `redeployVMs` provides the ability to redeploy the virtual hard drives of the source virtual machine to the virtual machines specified. This feature leverages the FlexClone feature on the controller as well.

The datastore management engine

The datastore management engine provides three methods for managing datastores: createDatastore, resizeDatastore, and destroyDatastore.

- The `createDatastore` method provides the ability to provision storage on the controller, present it to the ESX hosts, and create a datastore.
- The `resizeDatastore` method provides the ability to grow and shrink NFS-based datastores and grow VMFS-based datastores.
- The `destroyDatastore` method provides the ability to delete all virtual machines associated with the datastore, unmount it from ESX hosts, destroy the storage objects on the controller, and free the space.

The file copy/clone offload engine

The file copy/clone offload engine provides four methods. These methods provide the ability to execute and monitor file copy and clone operations.

This engine provides the ability to offload file copy and clone operations to the controller for NFS-based datastores. This functionality is unique compared to that provided by the other engines in that it does not require a Virtual Center session. An ESX host session can be used instead.

The input to the methods is a combination of complex (specification and message) and simple (string, int, long, boolean, and so on) data types. The specifications and messages are described below.

Note: Very little verification or validation is done in the API. For example, if there is not enough space to create the requested datastore(s), the API method will fail.

Provisioning and Cloning methods

This section describes all the available Provisioning and Cloning methods.

Virtual machine clone creation and redeploy engine

This section describes the APIs for interfacing with the virtual machine clone creation and redeploy engine.

createClones

You can use the `createClones` method to create virtual machine clones on new or existing datastores.

The source can be a virtual machine or a virtual machine template. The source can be further refined by specifying a virtual machine snapshot. The following options cause at least one native clone (built into Virtual Center) operation to occur:

- clone source is powered on
- virtual machine snapshot is specified
- hard drive transformation is specified

The virtual machine or template must not contain any RDMs, must not contain any devices that use `VMDirectPath`, and must be connected.

The mix of `VirtualIDEController` attached hard drives and `VirtualSCSIController` hard drives in the same virtual machine may result in the drives being reordered in the resulting clones, therefore this is not supported. The creation of virtual machines based on hardware version vmx-07 will fail on ESX 3.5 hosts.

Status

Current (added in version 2.1)

Type

Asynchronous

Parameters

Name	Type	Value	Description
requestSpec	Object	RequestSpec	Request can specify a vCenter server only. This method does not support direct connections to ESX hosts. **Note:** See *RequestSpec* on page 185.

XML

```
complexType name="createClones">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="arg0" type="{http://
server.kamino.netapp.com/}requestSpec" minOccurs="0"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

Returns

Type	Value	Description
String	`Task:task-2`	A managed object reference to a vCenter task. This task can be monitored and altered using the VI SDK

Return XML

```
<complexType name="createClonesResponse">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="return" type="{http://www.w3.org/
2001/XMLSchema}string" minOccurs="0"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

RedeployVMs

You can redeploy the virtual hard drives associated with a virtual machine to other virtual machines.

The source can be a virtual machine, a virtual machine template, or a virtual machine snapshot. The following options cause a native (built into Virtual Center) clone operation before it can use the rapid clone methodology:

- clone source is powered on
- virtual machine snapshot is specified
- hard drive transformation is specified

The virtual machine or template must not contain any RDMs or any devices that use `VMDirectPath`, and must be in a good state (connected).

Status

Current (added in version 3.0)

Type

Asynchronous

Parameters

Name	Type	Value	Description
requestSpec	Object	RequestSpec	**Note:** See *RequestSpec* on page 185.

XML

```
complexType name="redeployVMs">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="arg0" type="{http://
server.kamino.netapp.com/}requestSpec" minOccurs="0"/>
                <element name="arg1" type="{http://
server.kamino.netapp.com/}controllerSpec" maxOccurs="unbounded"
minOccurs="0"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

Returns

Type	Value	Description
String	`Task:task-2`	A managed object reference to a vCenter task. This task can be monitored and altered using the VI SDK

Return XML

```
<complexType name="redeployVMsResponse">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="return" type="{http://www.w3.org/
2001/XMLSchema}string" minOccurs="0"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

Datastore management engine

This section describes the APIs for interfacing with the datastore management engine.

createDatastore

You can use the `createDatastore` method to provision storage on the storage controller, attach it to one or more ESX hosts, and create a datastore.

More than one ESX host can be chosen by specifying the managed object reference of a cluster or datacenter in `DatastoreSpec`.

Status

Current (added in version 3.0)

Type

Synchronous

Parameters

Name	Type	Value	Description
dsSpec	Object	DatastoreSpec	The specification describing the datastore to create. **Note:** See *DatastoreSpec* on page 190.

Name	Type	Value	Description
policy	Object	policy	To use this parameter, you must have VASA Provider for clustered Data ONTAP installed and registered with VSC. This parameter supports the policy-based management feature of the VASA Provider and refers to a storage capability profile defined within the VASA Provider. When you use this parameter, it overrides any conflicting parameters defined within your datastore specification. For example, if you simultaneously include both NFS options and a policy option that specifies FCP, the FCP values associated with policy override the NFS options. As a result, VSC creates an FCP datastore. **Note:** VASA Provider and storage capability profiles are described in this guide.
requestSpec	Object	RequestSpec	Request can specify a vCenter server only. This method does not support direct connections to ESX hosts. **Note:** See *RequestSpec* on page 185.

XML

```
complexType name="createDatastore">
    <complexContent>
```

```
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="arg0" type="{http://
server.kamino.netapp.com/}requestSpec" minOccurs="0"/>
                <element name="arg1" type="{http://
server.kamino.netapp.com/}controllerSpec" minOccurs="0"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

Returns

Type	Value	Description
String	`newDatastore`	The name of the new datastore that was created.

Return XML

```
<complexType name="createDatastoreResponse">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="return" type="{http://www.w3.org/
2001/XMLSchema}string" minOccurs="0"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

resizeDatastore

You can use the `resizeDatastore` method to grow or shrink NFS-based datastores (and associated storage objects on the controller), and grow VMFS-based datastores (and associated storage objects on the controller).

Status

Current (added in version 3.0)

Type

Synchronous

Parameters

Name	Type	Value	Description
dsSpec	Object	DatastoreSpec	Specification describing datastore resize request.
requestSpec	Object	RequestSpec	Request can specify a vCenter server only. This method does not support direct connections to ESX hosts.

XML

```
complexType
name="resizeDatastore"
>
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="arg0" type="{http://
server.kamino.netapp.com/}requestSpec" minOccurs="0"/>
                <element name="arg1" type="{http://
server.kamino.netapp.com/}datastoreSpec" minOccurs="0"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

Returns

Type	Value	Description
String	`Task:task-2`	A managed object reference to a vCenter task.

Return XML

```
complexType name="resizeDatastoreResponse">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="return" type="{http://www.w3.org/
2001/XMLSchema}string" minOccurs="0"/>
```

```
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

destroyDatastore

You can use the `destroyDatastore` method to delete any virtual machine with a file on the specified datastore, delete the datastore (after detaching from each ESX host), take the storage objects offline, and destroy the datastore (to free space).

Status

Current (added in version 3.0)

Type

Synchronous

Parameters

Name	Type	Value	Description
dsSpec	Object	DatastoreSpec	Specification describing datastore resize request. **Note:** See *DatastoreSpec* on page 190.
requestSpec	Object	RequestSpec	Request can specify a vCenter server only. This method does not support direct connections to ESX hosts. **Note:** See *RequestSpec* on page 185.

XML

```
complexType name="destroyDatastore">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
```

```
XMLSchema}anyType">
            <sequence>
                <element name="arg0" type="{http://
server.kamino.netapp.com/}datastoreSpec" minOccurs="0"/>
                <element name="arg1" type="{http://
server.kamino.netapp.com/}requestSpec" minOccurs="0"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

Returns

Type	Value	Description
String	`Task:task-2`	A managed object reference to a vCenter task.

Return XML

```
<complexType name="destroyDatastoreResponse">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="return" type="{http://www.w3.org/
2001/XMLSchema}string" minOccurs="0"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

Connection Broker features

This section describes the APIs for interfacing with connection broker features.

performViewImport

You can use the `performViewImport` method to import the specified virtual machines into a VMware View Server.

Status

Current (added in version 3.2)

Type

Synchronous

Parameters

Name	Type	Value	Description
dsSpec	Object	DatastoreSpec	The specification describing the connection broker information.
requestSpec	Object	RequestSpec	Request can specify a vCenter server only. This method does not support direct connections to ESX hosts.
vmsForImport	List <String>		A list of the virtual machines (by name) that should be imported into the View server.

XML

```
complexType name="createDatastore">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="arg0" type="{http://
server.kamino.netapp.com/}connectionBrokerSpec" minOccurs="0"/>
                <element name="arg1" type="{http://
server.kamino.netapp.com/}requestSpec" minOccurs="0"/>
                <element name="arg2" type="{http://
server.kamino.netapp.com/}vmsForImport" minOccurs="0"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

Returns

Type	Value	Description
Void	N/A	Nothing returned

Return XML

```
complexType name="createDatastore">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="return" type="{http://www.w3.org/
2001/XMLSchema}void" minOccurs="0"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

createXenImportFile

You can use the `createXenImportFile` method to create a file for importing virtual machines into a Citrix XenDesktop server.

Status

Current (added in version 3.2)

Type

Synchronous

Parameters

Name	Type	Value	Description
dsSpec	Object	ConnectionBrokerSpec	The specification describing the connection broker information.
requestSpec	Object	RequestSpec	Request can specify a vCenter server only. This method does not support direct connections to ESX hosts.
vmsForImport	List		A list of the virtual machines (by name) that should be imported into the View server.

XML

```
complexType name="createXenImportFile">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="arg0" type="{http://
server.kamino.netapp.com/}connectionBrokerSpec" minOccurs="0"/>
                <element name="arg1" type="{http://
server.kamino.netapp.com/}requestSpec" minOccurs="0"/>
                <element name="arg2" type="{http://
server.kamino.netapp.com/}vmsForImport" minOccurs="0"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

Returns

Type	Value	Description
Void	N/A	Nothing returned

Return XML

```
complexType name="createXenImportFileResponse">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="return" type="{http://www.w3.org/
2001/XMLSchema}void" minOccurs="0"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

Copy/Clone offload engine

This section describes the APIs for interfacing with the Copy/Clone offload engine.

The `fileCopyOffload` and `fileCloneOffload` take VmFileSpec and RequestSpec as arguments. The `DatastoreSpec` should contain only the datastore-managed object reference and a reference to the controller. This is defined as *Existing Datastore* in the formulas section of the *DatastoreSpec* documentation.

fileCopyOffload

You can use the `fileCopyOffload` method to offload the copy of an NFS datastore file to the controller. This method should be used in cases where a full copy (all unique blocks) is required. In all other cases, the `fileCloneOffload` should be used.

This process involves a start-up time, which is quickly recovered when copying large files (because the offloaded controller base copy is very efficient). This start-up time may cause the offloaded copy of small files to take longer than using a host-based copy.

This method supports copying a file within the same controller. The VmFileSpec for the source and destination must specify the same controller.

Status

Current (added in version 3.0)

Type

Asynchronous

Parameters

Name	Type	Value	Description
source	Object	VmFileSpec	Specification describing the source file (datastore and controller).
destination	Object	VmFileSpec	Specification describing the destination file (datastore and controller).
requestSpec	Object	RequestSpec	Request can specify a vCenter server or ESX host.

XML

```
complexType name="fileCopyOffload">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="arg0" type="{http://
```

```
server.kamino.netapp.com/}vmFileSpec" minOccurs="0"/>
                <element name="arg1" type="{http://
server.kamino.netapp.com/}vmFileSpec" minOccurs="0"/>
                <element name="arg2" type="{http://
server.kamino.netapp.com/}requestSpec" minOccurs="0"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

Returns

Type	Value	Description
Integer	`876234`	The operation identifier to monitor using `getFileOpOffloadStatus`.

Return XML

```
complexType name="fileCopyOffloadResponse">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="return" type="{http://www.w3.org/
2001/XMLSchema}int/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

fileCloneOffload

You can use the `fileCloneOffload` method to offload the clone of an NFS datastore file to the controller.

This process uses the file level FlexClone feature of the controller. This process automatically falls back to the controller offloaded copy as needed if the fallBackToCopy parameter is set to `true`.

This method supports only cloning the file within the same volume. If fallBackToCopy is set to `true`, this method supports copying file within the same controller. In both cases, the `VmFileSpec` for the source and destination must specify the same controller.

The most effective use of this method is to employ a strategy where the output of the first operation (the destination file) becomes the input (the source file) for the next operation. For example, to create three clones of `test-flat.vmdk`, the following process (pseudo code) is the most efficient:

```
clone(test-flat.vmdk,test1-flat.vmdk)
clone(test1-flat.vmdk,test2-flat.vmdk)
clone(test2-flat.vmdk,test3-flat.vmdk)
```

Status

Current (added in version 3.0)

Type

Asynchronous

Parameters

Name	Type	Value	Description
source	Object	VmFileSpec	Specification describing the source file (datastore and controller).
destination	Object	VmFileSpec	Specification describing the destination file (datastore and controller).
fallBackToCopy	Boolean		If set to `true`, engine runs in "fully automatic mode" which falls back to an offloaded copy as needed. If `false`, conditions that would normally fall back to a copy result in an error (which the caller must deal with).
requestSpec	Object	RequestSpec	Request can specify a vCenter server or ESX host.

XML

```
complexType name="fileCloneOffload">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="arg0" type="{http://
server.kamino.netapp.com/}vmFileSpec" minOccurs="0"/>
                <element name="arg1" type="{http://
server.kamino.netapp.com/}vmFileSpec" minOccurs="0"/>
                <element name="arg2" type="{http://
server.kamino.netapp.com/}requestSpec" minOccurs="0"/>
                <element name="arg3" type="{http://www.w3.org/2001/
XMLSchema}boolean" minOccurs="0"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

Returns

Type	Value	Description
Integer	`876234`	The operation identifier to monitor using `getFileOpOffloadStatus`.

Return XML

```
complexType name="fileCloneOffloadResponse">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="return" type="{http://www.w3.org/
2001/XMLSchema}int/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

getFileOpOffloadStatus

You can use the `getFileOpOffloadStatus` method to track the progress of a `fileCopyOffload` or `fileCloneOffload` operation.

The status will be `complete`, `failed`, or `running`. When this method returns a StatusMessage with a status of `complete` or `failed`, the operation information is marked for cleanup, which occurs five minutes later. After the operation information has been cleaned up, it is no longer visible using this method. The progress field displays information about the progress of the operation.

Status

Current (added in version 3.0)

Type

Synchronous

Parameters

Name	Type	Value	Description
opId	Integer	`876234`	The operation identifier returned from `fileCopyOffload` or `fileCloneOffload`.

XML

```
complexType name="getFileOpOffloadStatus">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="arg0" type="{http://www.w3.org/2001/
XMLSchema}int"/>/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

Returns

Type	Value	Description
String	StatusMessage	Information describing status, progress, and reason for error (if operation fails). **Note:** See *StatusMessage* on page 199.

Return XML

```
complexType name="getFileOpOffloadStatusResponse">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="return" type="{http://
server.kamino.netapp.com/}statusMessage" minOccurs="0"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

clearAllFinishedOpOffloadStatus

You can use the `clearAllFinishedOpOffloadStatus` method to start the cleanup timer described in `getFileOpOffloadStatus` for all operations that have a status of `complete` or `failed`.

Status

Current (added in version 3.0)

Type

Synchronous

Parameters

Name	Type	Value	Description
opId	Integer		The operation identifier returned from `fileCopyOffload` or `fileCloneOffload`.

XML

```
complexType name="clearAllFinishedOpOffloadStatus">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

Returns

Void

Return XML

```
complexType name="clearAllFinishedOpOffloadStatusResponse">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

Utility methods

This section describes utility methods that return output, such as a list of created virtual machines and the managed object reference of each virtual machine.

getVms

You can use the `getVms` method to obtain the list of virtual machines that were created using the `createClones` method. This list can be used in the `redeployVMs` method.

Status

Current (added in version 3.0)

Type

Synchronous

Parameters

Name	Type	Value	Description
vmMorRef	Object	The managed object reference of the VM.	The managed object reference of the VM.

XML

```
complexType
name="getVms"
>
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="arg0" type="{http://www.w3.org/2001/
XMLSchema}string" minOccurs="0"/>
                <element name="arg1" type="{http://
server.kamino.netapp.com/}requestSpec" minOccurs="0"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

Returns

Type	Value	Description
vmMorRef	String	The managed object reference of the VM.
requestSpec	RequestSpec	Request can specify a vCenter server or ESX host.

Return XML

```
<complexType name="getVmsResponse">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="return" type="{http://www.w3.org/
2001/XMLSchema}string" maxOccurs="unbounded" minOccurs="0"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

getVmFiles

You can use the `getVmFiles` method to obtain a skeleton list of `VmFileSpec` to be completed and used in the submission to `createClones`.

Status

Current (added in version 2.1)

Type

Synchronous

Parameters

Name	Type	Value	Description
vmMorRef	String		The managed object reference of the VM.
requestSpec	Object	RequestSpec	Request can specify a vCenter server or ESX host.

XML

```
complexType
name="getVmFiles"
>
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="arg0" type="{http://www.w3.org/2001/
XMLSchema}string" minOccurs="0"/>
                <element name="arg1" type="{http://
server.kamino.netapp.com/}requestSpec" minOccurs="0"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

Returns

Type	Value	Description
List	Object <VmFileSpec>	A list of VmFileSpec based on the VM specified. This information should be modified and submitted using the CloneSpec.

Return XML

```
<complexType name="getVmFilesResponse">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="return" type="{http://
server.kamino.netapp.com/}vmFileSpec" maxOccurs="unbounded"
minOccurs="0"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

getMoref

You can use the getMoref method to obtain the managed object reference of the requested object based on name and type.

The getMoref method returns the first object that matches the name and type combination. For this reason, this method should not be used in production environments unless all object names are unique.

Status

Current (added in version 2.1)

Type

Synchronous

Parameters

Name	Type	Value	Description
name	String		Name of object to look for.

Name	Type	Value	Description
type	String		Managed object type.
requestSpec	String		Request can specify a vCenter server or ESX host.

XML

```
complexType
name="getMoref"
>
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="arg0" type="{http://www.w3.org/2001/
XMLSchema}string" minOccurs="0"/>
                <element name="arg1" type="{http://www.w3.org/2001/
XMLSchema}string" minOccurs="0"/>
                <element name="arg2" type="{http://
server.kamino.netapp.com/}requestSpec" minOccurs="0"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

Returns

Type	Value	Description
String		Managed object reference in string format.

Return XML

```
<complexType name="getMorefResponse">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="return" type="{http://www.w3.org/
2001/XMLSchema}string" minOccurs="0"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

Provisioning and Cloning specifications and messages

The Provisioning and Cloning API provides several specifications and messages.

RequestSpec

The `RequestSpec` specification describes the URL of the VMware vCenter SDK or ESX host as well as the authentication information. The authentication information may be in the form of a user name and password combination or a VMware Session ID. An optional clone specification may also be present.

Properties

Type	Value	Description
serviceUrl	String	URL for the VMware vCenter SDK
vcUser	String	VMware vCenter username (null ok if using vcSession)
vcPassword	String	VMware vCenter password (null ok if using vcSession)
vcSession	String	VMware session (null ok if using vcUser/vcPassword)
cloneSpec	Object `CloneSpec`	A clone specification

Notes

- cloneSpec may be null when using this spec with anything other than `redeployVMs` or `createClones`.
- vcSession should be null if vcUser and vcPassword are used.
- vcUser and vcPassword should be `null` if vcSession is used.

XML

```
complexType
name="requestSpec"
>
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="cloneSpec" type="{http://
server.netapp.com/}cloneSpec" minOccurs="0"/>
```

```
                <element name="serviceUrl" type="{http://www.w3.org/
2001/XMLSchema}string" minOccurs="0"/>
                <element name="vcPassword" type="{http://www.w3.org/
2001/XMLSchema}string" minOccurs="0"/>
                <element name="vcSession" type="{http://www.w3.org/
2001/XMLSchema}string" minOccurs="0"/>
                <element name="vcUser" type="{http://www.w3.org/
2001/XMLSchema}string" minOccurs="0"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

CloneSpec

The `CloneSpec` specification describes a request to create clones of a virtual machine or template or to redeploy the virtual hard drives.

When used with the `redeployVMs` method, each virtual machine in the map named clones will have its virtual hard drives replaced with those of the source. The string in this map is the name of the virtual machine to be redeployed and the `VmSpec` describes this virtual machine.

When `CloneSpec` is used with the `createClones` method, a new virtual machine is created for each entry in the clones map. The string in this map is the name of the clone and the `VmSpec` describes the new clone configuration. The list named files describes the files that make up the source virtual machine or template. This list can be used to specify different destinations for each file as well as to create new datastores.

Type	Value	Description
templateMoref	String	Source VM or template of cloning operation. String representation of type and value of ManagedObjectReference from VMware VI API.
snapshotMoref	String	The managed object reference for a snapshot of the source virtual machine to base the clones on.

Type	Value	Description
containerMoref	String	Destination for resulting clones. Valid destination types: `Datacenter`, `ResourcePool`, `ClusterComputeResource`, and `ComputeResource`, A string representation of type and value of ManagedObjectReference from the VMware VI API.
destVmFolderMoref	String	Virtual machine folder the clones should be created in. If `null`, clones are created at the root virtual machine folder.
vmTransform	String	Transforms all virtual hard drives to specified format. Should be specified only when there is actual work to do. Specifying a transform when one is not required causes unnecessary work. Options are `null`, `flat`, and `sparse`.
hardwareVersion	String	Upgrade hardware version from a previous version to vmx-04 or vmx-07. **Note:** vmx-04 is supported by ESX 3.5 and both are supported by ESX 4.0.
clones	Map <String, VmSpec>	Map of new virtual machine name to virtual machine specification (VmSpec).
files	List <VmFileSpec>	List of files that make up source virtual machine or template specified in templateMoref.
memMB	Long	Override the source virtual machine (or template) amount of memory during cloning process. Value is in MB.

Type	Value	Description
numberCPU	Int	Override the source virtual machine (or template) number of CPUs during cloning process.

XML

```
<complexType name="cloneSpec">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="clones">
                    <complexType>
                        <complexContent>
                            <restriction base="{http://www.w3.org/
2001/XMLSchema}anyType">
                                <sequence><element name="entry"
maxOccurs="unbounded" minOccurs="0">
                                    <complexType>
                                        <complexContent>
                                            <restriction
base="{http://www.w3.org/2001/XMLSchema}anyType">
                                                <sequence>
                                                    <element
name="key" type="{http://www.w3.org/2001/XMLSchema}string"
minOccurs="0"/>
                                                    <element
name="value" type="{http://server.netapp.com/}vmSpec"
minOccurs="0"/>
                                                </sequence>
                                            </restriction>
                                        </complexContent>
                                    </complexType>
                                </element>
                            </sequence>
                        </restriction>
                    </complexContent>
                </complexType>
            </element>
            <element name="connBroker" type="{http://
server.netapp.com/}connectionBrokerSpec" minOccurs="0"/>
            <element name="containerMoref" type="{http://www.w3.org/
2001/XMLSchema}string" minOccurs="0"/>
            <element name="destVmFolderMoref" type="{http://
www.w3.org/2001/XMLSchema}string" minOccurs="0"/>
            <element name="files" type="{http://
server.kamino.netapp.com/}vmFileSpec" maxOccurs="unbounded"
minOccurs="0"/>
            <element name="hardwareVersion" type="{http://
www.w3.org/2001/XMLSchema}string" minOccurs="0"/>
            <element name="snapshotMoref" type="{http://www.w3.org/
```

```
2001/XMLSchema}string" minOccurs="0"/
>
            <element name="templateMoref" type="{http://www.w3.org/
2001/XMLSchema}string" minOccurs="0"/>
            <element name="vmTransform" type="{http://www.w3.org/
2001/XMLSchema}string" minOccurs="0"/>
            <element name="memMB" type="{http://www.w3.org/2001/
XMLSchema}long" minOccurs="0"/>
            <element name="numberCPU" type="{http://www.w3.org/2001/
XMLSchema}int" minOccurs="0"/>
        </sequence>
    </restriction>
</complexContent>
</complexType>
```

VmFileSpec

The `VmFileSpec` specification describes the source configuration file (`vmx`) or the source virtual hard disk files (`vmdk`) as well as the destination datastore specification.

Properties

Type	Value	Description
sourcePath	String	Path to `vmx` or `vmdk` file. The string Configuration File can be passed in place of an actual `vmx` file.
destDatastoreSpec	DatastoreSpec	Destination datastore specification.

XML

```
<complexType name="vmFileSpec">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="destDatastoreSpec" type="{http://
server.netapp.com/}datastoreSpec" minOccurs="0"/>
                <element name="sourcePath" type="{http://www.w3.org/
2001/XMLSchema}string" minOccurs="0"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

DatastoreSpec

The `DatastoreSpec` specification describes the destination datastore. This can describe new datastores to be created as well as existing datastores.

See the "Required parameters" section below for valid parameter combinations. The number of clones must be evenly divisible by the number of datastores.

Properties

Type	Value	Description
mor	String	Destination datastore. String representation of type and value of `ManagedObjectReference` from the VMware VI API.
targetMor	String	The managed object reference of the vCenter object in which to attach the new datastore. Can be an ESX host, cluster or datacenter.
goldVolume	String	Name of volume used when creating more than one NFS-based datastore. This volume is not permanently presented to the ESX hosts. This volume becomes the parent of the FlexClones.
protocol	String	The protocol being used. Valid values are NFS, FCP, iSCSI.
containerName	String	Name of the aggregate for new NFS datastores, or name of volume for new VMFS datastores.
sizeInMB	Long	Size of the datastore in MB. An additional 256 MB is added for VMFS datastores to cover metadata overhead.

Type	**Value**	**Description**
thinProvision	Boolean	If `true`, space will not be reserved for the storage object. For NFS, the volume will guarantee=`none`. For VMFS, LUN will be created with '-o noreserve'.
volAutoGrow	Boolean	If `true`, the volAutoGrowInc and volAutoGrowMax values are applied to the volume.
volAutoGrowInc	Long	Increment in which to grow volume automatically as needed in MB.
volAutoGrowMax	Long	Maximum size to which to grow the volume automatically in MB.
datastoreNames	List <String>	List of datastore names. Care should be taken by the application to prevent duplicate datastore, volume or LUN names. For NFS, datastore name is used as volume name. For VMFS, datastore name is used as LUN name.
numDatastores	Int	Number of datastores. This should indicate the size of the list of names in datastoreNames.
blockSize	Int	VMFS block size in MB.
controller	ControllerSpec	The controller.

Type	Value	Description
wrapperVol	Boolean	When `true`, new volume is created to contain the new LUN to be used for a new VMFS datastore (containerName must contain aggregate name if `true`). When `true`, the volume containing the LUN (VMFS datastore) will be resized to make room for the new size of the LUN (if required).

Required parameters

Some actions require the use of multiple parameters.

Specifying an existing datastore

- mor
- controller

Specifying new NFS datastores using createClones or createDatastore

- targetMor - only required for `createDatastore`
- containerName
- sizeInMB
- thinProvision
- volAutoGrow
- volAutoGrowInc
- volAutoGrowMax
- protocol - must be NFS
- controller
- datastoreNames - only one name in the list
- numDatastores - should be 1

Specifying new NFS datastores using createClones

- goldVolume
- containerName
- sizeInMB
- thinProvision
- volAutoGrow
- volAutoGrowInc

- volAutoGrowMax
- protocol - Must be NFS
- controller
- datastoreNames
- numDatastores

Specifying new VMFS datastores using createClones or createDatastore

- targetMor - only required for `createDatastore`
- containerName
- sizeInMB
- thinProvision
- protocol - must be FCP or iSCSI
- controller
- datastoreNames - only one name in the list
- numDatastores - should be 1

Specifying new VMFS datastores using createClones

- containerName
- sizeInMB
- thinProvision
- protocol - must be FCP or iSCSI
- controller
- datastoreNames
- numDatastores

XML

```
<complexType name="datastoreSpec">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/XMLSchema}anyType">
            <sequence>
                <element name="containerName" type="{http://www.w3.org/
2001/XMLSchema}string" minOccurs="0"/>
                <element name="blockSize" type="{http://www.w3.org/2001/
XMLSchema}int" minOccurs="0"/>
                <element name="controller" type="{http://
server.kamino.netapp.com/}controllerSpec" minOccurs="0"/>
                <element name="datastoreNames" type="{http://www.w3.org/
2001/XMLSchema}string" maxOccurs="unbounded" minOccurs="0"/>
                <element name="goldVolume" type="{http://www.w3.org/2001/
XMLSchema}string" minOccurs="0"/>
                <element name="mor" type="{http://www.w3.org/2001/
XMLSchema}string" minOccurs="0"/>
                <element name="numDatastores" type="{http://www.w3.org/
2001/XMLSchema}int"/>
```

```
                <element name="protocol" type="{http://www.w3.org/2001/
XMLSchema}string" minOccurs="0"/>
                <element name="sizeInMB" type="{http://www.w3.org/2001/
XMLSchema}long" minOccurs="0"/>
                <element name="targetMor" type="{http://www.w3.org/2001/
XMLSchema}string" minOccurs="0"/>
                <element name="temp" type="{http://www.w3.org/2001/
XMLSchema}string" minOccurs="0"/>
                <element name="thinProvision" type="{http://www.w3.org/
2001/XMLSchema}boolean"/>
                <element name="volAutoGrow" type="{http://www.w3.org/
2001/XMLSchema}boolean"/>
                <element name="volAutoGrowInc" type="{http://www.w3.org/
2001/XMLSchema}long" minOccurs="0"/>
                <element name="volAutoGrowMax" type="{http://www.w3.org/
2001/XMLSchema}long" minOccurs="0"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

ControllerSpec

The `ControllerSpec` specification describes the controller connection and authentication data. This information is used by the VSC provisioning and cloning features to connect to the controller using the ZAPI interface. No other protocol is used to connect to the controller.

Properties

Type	Value	Description
ipAddress	String	IP or host name of the controller.
username	String	User name (does not need to be root).
password	String	Password.
ssl	Boolean	If `true`, use HTTPS. If `false`, use HTTP to connect to the controller.
passthroughContext	String (optional)	Name of the vFiler or Storage Virtual Machine (SVM, formerly known as Vserver) on which to create the new storage.

Type	Value	Description
actuallyOpsMgr	Boolean (optional)	If `true`, connects to Operations Manager. If `false`, connects to controller.

XML

```
<complexType name="controllerSpec">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="ipAddress" type="{http://www.w3.org/
2001/XMLSchema}string" minOccurs="0"/>
                <element name="password" type="{http://www.w3.org/
2001/XMLSchema}string" minOccurs="0"/>
                <element name="ssl" type="{http://www.w3.org/2001/
XMLSchema}boolean"/>
                <element name="username" type="{http://www.w3.org/
2001/XMLSchema}string" minOccurs="0"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

VmSpec

The `VmSpec` specification describes configuration and action options for each virtual machine created.

The MAC address must be in a range defined by VMware. Refer to VMware documentation for more information.

Properties

Type	Value	Description
macAddress	Map <String, String>	Virtual network adapter to MAC address information (optional).
custSpecName	String	Name of guest customization specification to be applied (optional).
vmMoref	String	The managed object reference of the virtual machine to be redeployed.

Type	Value	Description
powerOn	Boolean	If `true`, the new virtual machines are powered on after all have been created.

XML

```
<complexType name="vmSpec">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="custSpec" type="{http://
server.kamino.netapp.com/}guestCustomizationSpec" minOccurs="0"/>
                <element name="domain" type="{http://
server.kamino.netapp.com/}domainSpec" minOccurs="0"/>
                <element name="macAddress">
                    <complexType>
                        <complexContent>
                            <restriction base="{http://www.w3.org/
2001/XMLSchema}anyType">
                                <sequence>
                                    <element name="entry"
maxOccurs="unbounded" minOccurs="0">
                                        <complexType>
                                            <complexContent>
                                                <restriction
base="{http://www.w3.org/2001/XMLSchema}anyType">
                                                    <sequence>
                                                        <element
name="key" type="{http://www.w3.org/2001/XMLSchema}string"
minOccurs="0"/>
                                                        <element
name="value" type="{http://www.w3.org/2001/XMLSchema}string"
minOccurs="0"/>
                                                    </sequence>
                                                </restriction>
                                            </complexContent>
                                        </complexType>
                                    </element>
                                </sequence>
                            </restriction>
                        </complexContent>
                    </complexType>
                </element>
                <element name="powerOn" type="{http://www.w3.org/
2001/XMLSchema}boolean"/>
                <element name="vmMoref" type="{http://www.w3.org/
2001/XMLSchema}string" minOccurs="0"/>
            </sequence>
        </restriction>
```

```
    </complexContent>
</complexType>
```

GuestCustomizationSpec

The `GuestCustomizationSpec` specification identifies the guest customization specification.

Properties

Type	Value	Description
name	String	Name of the guest customization specification.
useVmName	Boolean	If guest customization specification is of type `CustomizationSysprepText`, this option can be used to make the guest hostname match the virtual machine name. **Note:** It is the responsibility of the implementer to ensure that the virtual machine name results in a valid host name.

XML

```
<complexType name="guestCustomizationSpec">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="name" type="{http://www.w3.org/2001/
XMLSchema}string" minOccurs="0"/>
                <element name="useVmName" type="{http://www.w3.org/
2001/XMLSchema}boolean"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

ConnectionBrokerSpec

The `ConnectionBrokerSpec` specification describes the connection broker and authentication data. This information is used by VSC for VMware vSphere to connect to the connection broker (VMware View or Citrix XenDesktop).

Properties

Type	Value	Description
type	ConnectionBrokerType	The type of connection broker to import into. This can be `VMWARE_VIEW_4_0`, `VMWARE_VIEW_4_5`, or `XEN_DESKTOP`.
host	String	Hostname or IP address of the connection broker (used only for View import).
username	String	A user who can access the View Server (used only for View import).
password	String	Password of the specified user (used only for View import).
domain	String	FQDN where the connection broker resides.
desktopType	DesktopType	`INDIVIDUAL_DESKTOP` or `DESKTOP_POOL` (used only for View import).
accessMode	AccessMode	`PERSISTENT` or `NON_PERSISTENT`. This corresponds to dedicated and floating in View 4.5 and higher, respectively (used only for View import).
poolType	PoolType	`NEW` or `EXISTING`. Create a new pool or use an existing one (used only for View import).
poolName	String	The name of the new pool if the PoolType is set to `NEW` (used only for View import).

StatusMessage

You can use the `StatusMessage` specification to obtain the progress and status of an operation.

Properties

Type	Value	Description
id	Int	Operation identifier.
progress	Int	Valid values are 0-100. Indicates how much of the copy or clone process has completed at the time of the query.
status	String	Valid values are `complete` (finished without error), `failed` (finished with error), or `running` (operation in progress).
reason	String	If the status is `failed`, this contains the reason for the failure.

XML

```
<complexType name="statusMessage">
    <complexContent>
        <restriction base="{http://www.w3.org/2001/
XMLSchema}anyType">
            <sequence>
                <element name="id" type="{http://www.w3.org/2001/
XMLSchema}int"/>
                <element name="progress" type="{http://www.w3.org/
2001/XMLSchema}int"/>
                <element name="reason" type="{http://www.w3.org/
2001/XMLSchema}string" minOccurs="0"/>
                <element name="status" type="{http://www.w3.org/
2001/XMLSchema}string" minOccurs="0"/>
            </sequence>
        </restriction>
    </complexContent>
</complexType>
```

Provisioning and Cloning sample code

```
<ns2:createClonesxmlns:ns2="http://server.kamino.netapp.com/">
<arg0>
    <cloneSpec>
        <clones>
            <entry>
                <key>apiTestClone1</key>
                <value>
                    <powerOn>false</powerOn>
                </value>
            </entry>
            <entry>
                <key>apiTestClone2</key>
                <value>
                    <powerOn>false</powerOn>
                </value>
            </entry>
            <entry>
                <key>apiTestClone3</key>
                <value>
                    <powerOn>false</powerOn>
                </value>
            </entry>
        </clones>
        <containerMoref>Datacenter:datacenter-2</containerMoref>
        <files>
            <destDatastoreSpec>
                <controller>
                    <ipAddress>10.10.10.2</ipAddress>
                    <password></password>
                    <ssl>false</ssl>
                    <username>root</username>
                </controller>
                <mor>Datastore:datastore-17</mor>
                <numDatastores>0</numDatastores>
                <thinProvision>false</thinProvision>
                <volAutoGrow>false</volAutoGrow>
            </destDatastoreSpec>
            <sourcePath>[unitTestSourceNFS]demoSource/
demoSource.vmx</sourcePath>
        </files>
        <files>
            <destDatastoreSpec>
                <controller>
                    <ipAddress>10.10.10.2</ipAddress>
                    <password></password>
                    <ssl>false</ssl>
                    <username>root</username>
                </controller>
                <mor>Datastore:datastore-17</mor>
                <numDatastores>0</numDatastores>
```

```
                <thinProvision>false</thinProvision>
                <volAutoGrow>false</volAutoGrow>
            </destDatastoreSpec>
            <sourcePath>[unitTestSourceNFS]demoSource/
demoSource.vmdk</sourcePath>
        </files>
        <templateMoref>VirtualMachine:vm-255</templateMoref>
    </cloneSpec>
    <serviceUrl>https://10.10.10.2/sdk</serviceUrl>
    <vcPassword>pass123</vcPassword>
    <vcUser>Administrator</vcUser>
</arg0>
</ns2:createClones>
```

Provisioning and Cloning client-side programming

Various client-side programming environments allow you to access the SOAP service. You can use this service for your own client-side programming.

Accessing the SOAP API through Java

You can access the SOAP API by using Java-based tools or the Java programming language.

Generating a certificate for use with the wsimport tool

You must generate a certificate for use with `wsimport` so that the tool will be able to read the WSDL that is generated by the build process.

About this task

Complete the following steps to generate a certificate for use with `wsimport`.

Steps

1. Stop the NVPF service. This step is optional if you have already generated an SSL certificate for the environment.
2. Run the following command in the VSC for VMware vSphere installation directory: `c:\Program Files\NetApp\Virtual Storage Console>bin\vsc ssl setup -domain <domain`

   For <*domain*>, enter the host name of the system running VSC for VMware vSphere or a fully qualified domain name of the system running VSC for VMware vSphere.

   Note: This step is optional if you have already generated an SSL certificate for the environment.

3. From the VSC for VMware vSphere installation directory, change to `\etc` and run the command: `keytool -export -alias nvpf -keystore nvpf.keystore -file nvpf.cer`

   Note: If you moved the keystore file from the `c:\Program Files\NetApp\Virtual Storage Console\etc` directory, enter the path to the keystore file.

   This command creates a new file called `nvpf.cer`.

   This certificate will be imported to the local Java keystore. If you have the Java JRE version 1.6.0_21 installed in Program Files, the command to execute will look like this:

   ```
   c:\Program Files\NetApp\Virtual Storage Console\etc>keytool -import -
   alias nvpf -file nvpf.cer -keystore "c:\Program Files\Java
   \jdk1.6.0_21\jre\lib\security\cacerts"
   ```

4. Enter keystore password:

   changeit

5. Run `wsimport` to grab the WSDL and generate the Java classes to write your own client. Enter the commands:

   cd \dev

   **c :\dev\wsimport -verbose -s . -p com.netapp.kamino.api https://
   <*domain*>:8143/kamino/public/api?wsdl**

   Be sure to change <*domain*> to a valid host or domain name. If that name does not resolve through DNS, add it to your hosts file (not localhost).

Accessing SOAP through C#

To begin using the SOAP API, you must first add the web reference to your project.

After the web service reference has been added, you can start accessing the client side objects to make API calls into the SOAP service.

Creating custom user accounts for backup and restore operations

You can override the default authentication method by creating a custom user account using the VSC CLI, which enables you to log in with user credentials other than your Windows credentials. A non-root or non-administrator account might be required to access a specific storage system.

You must create a custom storage system account with a new storage system role, group, and user as described in the following table.

Item	Description
Role	The new role must allow VSC to access the storage system data through its APIs.
Group	A storage system maintains groups as a collection of roles. The group you create must contain your new role.
User	A user account that VSC uses to access a storage system must be a member of a group that contains a role. You can create this user and assign a password to it, which enables you to add a storage system to VSC with the assigned user name and password.

For more information about how to manage users on your storage system, see your storage system's administrator guide.

Using the VSC CLI to create a custom user account

You can use the VSC CLI to create a custom user account. The user credentials for a custom user account provide the same access to commands and features as an administrator who logs in using the default Windows credentials authentication method.

Steps

1. Double-click the **VSC CLI** desktop icon or navigate to **Start > All Programs > NetApp > Virtual Storage Console > VSC CLI**.
2. Enter the following command:

   ```
   smvi servercredential set
   ```

3. Specify a user name and a password for this user account.

Using the VSC CLI to create a custom user account for a storage system

You can use the command line of your storage system to create a custom storage system account with a new role, group, and user for the storage system.

About this task

The following steps are performed from the command line of the storage system that VSC needs to access.

Steps

1. Create a role named api-access with the minimum configuration required for VSC to access the storage system:

   ```
   useradmin role add api-access -a api-*,login-http-admin,cli-ifconfig
   ```

2. Create a group named api-group that contains the api-access role:

   ```
   useradmin group add api-group -r api-access
   ```

3. Create a user named smvi-user as a member of the api-group group:

   ```
   useradmin user add smvi-user -g api-group
   ```

4. Set the user password by running the `passwd` command as root.

   The storage system prompts you for the account name that you want to change, followed by the new password for this account.

VSC CLI commands

The VSC for VMware vSphere command-line interface (CLI), which is labeled "VSC CLI" on your Windows desktop, provides you the benefits of a command-based view of the user interface. You can use this CLI to perform specific Backup and Recovery tasks, such as creating or deleting a backup of a virtual machine or datastore, as well as mounting a backup.

You should keep in mind the following information about the commands that you see in the interface:

- Virtual Storage Console commands are case-sensitive.
- There are no privilege levels; any user with a valid user name and password can run all commands.

For some commands, the following two parameters control the amount of output displayed:

verbose This optional parameter provides detailed output when displaying information.

quiet This optional parameter stops any output from displaying.

Note: Even with the quiet parameter specified, failed commands still display their failure messages.

Launching the VSC CLI

You can use either of two methods to launch the VS for VMware vSphere command-line interface (CLI), which is labeled "VSC CLI" on your Windows desktop. The first time you launch the VSC CLI, the application uses your Windows user credentials to grant you server access. Subsequent launches use stored credentials, speeding your access to the server.

About this task

When you issue your first CLI command, the CLI prompts you for your password and then runs the command. If the command succeeds, the CLI caches your user credentials and stores the information locally in an encrypted format.

Step

1. Double-click the **VSC CLI** icon or navigate to **Start > All Programs > NetApp > VSC CLI**.

   An alternative method to using your Windows user credentials is to use the `smvi servercredential set` command to create custom user credentials that allow you to log in to the server.

smvi backup create

The `smvi backup create` command creates a backup copy of a virtual machine or datastore. You can also perform this operation using the VSC for VMware vSphere user interface.

Syntax

```
smvi backup create    [-id {name | id} [name | id ...]    [-backup-name
{backup name}]    [-server {server name}]    [-include-independent] [-
exclude-datastores {name | id} [name | id ...] [-scripts {script name}]
[-vmware-snapshot] [-no-vmware-snapshot] [-update-mirror] [-allow-vault]
[-quiet]    [-verbose]    [-user]    [-help]
```

Parameters

[-id {*name* | *id*}] [*name* | *id* ...]

This mandatory parameter specifies the name or identification of the datastore or virtual machine that you are backing up. You can specify names or identifications of multiple datastores or virtual machines.

[-backup-name {*backup name*}]

This optional parameter specifies a backup copy name. After adding the flag, add a name for the backup copy. If you specify no name with this flag, the command fails. If you specify a name that contains only spaces, VSC for VMware vSphere automatically generates a name. If you specify a name that contains both spaces and other characters, VSC for VMware vSphere removes all leading and trailing spaces from the name.

[-server {*server name*}]

This optional parameter specifies the name of the SnapManager for Virtual Infrastructure server to which you are sending this command. The default value is localhost.

[-include-independent]

This optional parameter specifies that datastores containing only independent disks for a virtual machine are included in the backup job.

[-exclude-datastores {*name* | *id*}] [*name* | *id* ...]

This optional parameter specifies the name or identification of the datastores or virtual machines to be excluded from the backup job.

[-scripts {*script name*}]

This optional parameter specifies the name of the scripts to run with this backup job.

[-vmware-snapshot]

This optional parameter creates VMware snapshots of virtual machines during a backup operation. If you specify this parameter along with [`-no-vmware-snapshot`], or if you do not specify either one of the parameters, it prevents the creation of any VMware snapshots.

[-no-vmware-snapshot]

This optional parameter prevents the creation of VMware snapshots of virtual machines during a backup operation.

[-update-mirror]

This optional parameter initiates a SnapMirror image on the secondary storage.

[-allow-vault]

This optional parameter initiates a SnapVault image on the secondary storage.

[-quiet]

This optional parameter stops any output from displaying.

[-verbose]

This optional parameter provides detailed output when displaying information.

[-user]

Add this optional parameter if you want to log in to the SnapManager for Virtual Infrastructure server with different credentials than you are currently logged in with.

[-help]

This optional parameter displays help for this command.

Example: Creating a backup copy from a virtual machine

The following example creates a backup copy from a virtual machine named testInd, without specifying a backup name:

```
smvi backup create -id testInd

[18:19] Starting backup request
[18:19] Backing up datastore(s)([DS_vee_cmode_03-04
(4fd6aad6-579ff358-676a-e41 f13ba10f6), nfs_cmode_test1 (netfs://
10.60.189.79///vol_nfs_test1)])
[18:19] Backing up the following virtual machine(s) ([testInd])
[18:20] Creating storage snapshots for all datastores/virtual
machines that are being backed up.
[18:20] Storing logs for backup_43e100cdf8182d1ee79bae431f1c608f in
file .\repos itory\logs\unscheduled
\backup_backup_43e100cdf8182d1ee79bae431f1c608f.xml
[18:20] Backup backup_43e100cdf8182d1ee79bae431f1c608f of
```

```
datastores/virtual machines is complete.
SMVICLI-0100: Command completed successfully
```

smvi backup delete

The `smvi backup delete` command removes a virtual machine or datastore backup copy. You can also perform this operation using the VSC for VMware vSphere user interface.

Syntax

```
smvi backup delete    -backup-name {backup name}    [-server {server
name}]    [-quiet]    [-verbose]    [-noprompt]    [-user]    [-help]
```

Description

When you delete the most recent backup associated with a backup job, then the Last Run Status value displayed for that backup job in the Schedule Backup Jobs window is that of the most recent remaining undeleted backup copy associated with the backup job.

Parameters

[-backup-name {*backup name*}]

This mandatory parameter specifies the backup copy you want to delete. After adding the flag, add the name of the backup copy.

[-server {*server name*}]

This optional parameter specifies the name of the SnapManager for Virtual Infrastructure server to which you are sending this command. The default value is localhost.

[-quiet]

This optional parameter stops any output from displaying.

[-verbose]

This optional parameter provides detailed output when displaying information.

[-noprompt]

This optional parameter disables the default prompt that asks for confirmation when deleting a backup.

[-user]

Add this optional parameter if you want to log in to the SnapManager for Virtual Infrastructure server with different credentials than you are currently logged in with.

[-help]

This optional parameter displays help for this command.

Example: Deleting a backup copy

The following example deletes a backup copy named new-one:

```
smvi backup delete -backup-name new-one

Are you sure you want to proceed and remove backup named 'new-one'?
[yes|NO] y
[15:15] Removed backup with name "new-one"
SMVICLI-0100: Command completed successfully
```

smvi backup list

The `smvi backup list` command displays information, such as the file path on a storage system to the Snapshot copy, about all of the created and saved backups within a virtual machine or datastore. You can also perform this operation using the VSC for VMware vSphere user interface.

Syntax

```
smvi backup list    [-id {name | id} [name | id ...]]    [-mounted] [-
failed] [-recent] [-with-vmware-snapshot] [-sfr-mounted]        [-server
{server name}]    [-user]    [-help]
```

Parameters

[-id {*name* | *id*} [*name* | *id* ...]]

This mandatory parameter specifies the name or identification of the datastores or virtual machines that you want to list.

[-mounted]

This optional parameter lists all mounted backups.

[-failed]

This optional parameter lists all failed backups. The default list is only successful backups.

[-recent]

This optional parameter lists the most recent backup.

[-with-vmware-snapshot]

This optional parameter lists the backups that were taken with a VMware snapshot.

[-sfr-mounted]

This optional parameter lists the backups that were mounted for SFR.

[-server {*server name*}]

This optional parameter specifies the name of the SnapManager for Virtual Infrastructure server to which you are sending this command. The default value is localhost.

[-user]

Add this optional parameter if you want to log in to the SnapManager for Virtual Infrastructure server with different credentials than you are currently logged in with.

[-help]

This optional parameter displays help for this command.

Example: Listing backups in a datastore

The following example lists all of the backups within a datastore named data-store1:

```
smvi backup list -id data-store01

Id Name Date Entities Mounted VMware Snapshot Snapshot Name
-------- -------------------- --------------------
-------------------- -------- ---------------- -------------
   backup_sch_1_20090122233100 Jan 22, 2009 23:31 vmfs_vm1 No
10.72.248.38:/vol/kas1_102_iscsi:smvi_backup_sch_1
20090122233100_36d2d99a-9ee0-4841-80c0-846698463e78_kas_sw_iscsi_ds1
```

smvi backup mount

The `smvi backup mount` command mounts a backup so that you can verify its contents.

Syntax

```
smvi backup mount    -backup-name {backup name}    -esx-server {esx
server name}    [-server {server name}]    [-quiet]    [-verbose]    [-
user]    [-help]
```

Privilege level

Note: To mount a VMFS datastore backup, the supplied ESX server must have SAN or iSAN access to the storage system, including required FC zoning or iSCSI discovery. To mount an NFS datastore backup, the supplied ESX server must be in the NFS export list of the original datastore.

Parameters

[-backup-name {*backup name*}]

This mandatory parameter specifies the backup you want to mount. After adding the flag, add the name of the backup.

[-esx-server {*esx server name* | *IP address*}]

This mandatory parameter specifies the name or IP address of the ESX server. This information describes where the backup resides on an ESX server.

Note: The server name is the name of the ESX server as viewed through the vSphere Client. This name might differ from the ESX server's host name or IP address.

[-server {*server name*}]

This optional parameter specifies the name of the SnapManager for Virtual Infrastructure server to which you are sending this command. The default value is localhost.

[-quiet]

This optional parameter stops any output from displaying.

[-verbose]

This optional parameter provides detailed output when displaying information.

[-user]

Add this optional parameter if you want to log in to the SnapManager for Virtual Infrastructure server with different credentials than you are currently logged in with.

[-help]

This optional parameter displays help for this command.

Example: Mounting a backup

The following example mounts a backup named vmfs2_vm1 on an ESX server with the IP address of 123.12.1.23:

```
smvi backup mount -backup-name vmfs2_vm1 -esx-server 123.12.1.23
```

```
[12:12] Starting mount request
SMVICLI-0100: Command completed successfully
```

smvi backup rename

The `smvi backup rename` command changes the name of a backup. Changing the name of a backup also changes the name on the corresponding storage Snapshot copy on the associated NetApp storage system. You can also perform this operation using the VSC for VMware vSphere user interface.

Syntax

```
smvi backup rename -backup-name {backup name} -new-backup-name {new name} [-server {server name}] [-user] [-help]
```

Parameters

[-backup-name {*backup name*}]

This mandatory parameter specifies the backup you want to rename. After adding the flag, add the name of the backup.

[-new-backup-name {*new name*}]

This mandatory parameter specifies the new name of the backup. After adding the flag, add a new name for the backup.

[-server-name {*server name*}]

This optional parameter specifies the name of the SnapManager for Virtual Infrastructure server to which you are sending this command.

[-user]

Add this optional parameter if you want to log in to the SnapManager for Virtual Infrastructure server with different credentials than you are currently logged in with.

[-help]

This optional parameter displays help for this command.

Example: Renaming a backup

The following example renames a backup named vmfs2-vm1 to volume-2:

```
smvi backup rename -backup-name vmfs2-vm1 -new-backup-name volume-2
```

```
[15:52] Backup "vmfs2-vm1" has been renamed to "volume-2"
SMVICLI-0100: Command completed successfully
```

smvi backup restore

The `smvi backup restore` command enables you to restore a virtual machine or datastore from a backup copy. You can also perform this operation using the VSC for VMware vSphere user interface.

Syntax

```
smvi backup restore    -id {name | id}    [-esx-server {esx server
name]    [-backup-name {backup name}]    [-vmdk {hard disk name}] [-
server {server name}]  [-restart-vm]    [-quiet]    [-verbose]    [-
noprompt]    [-user]    [-help]
```

Parameters

[-id {*name* | *id*}]

This mandatory parameter specifies the name or identification of the datastore or virtual machine that you are restoring.

[-esx-server {*esx server name* | *IP address*}]

This mandatory parameter specifies the name or IP address of the ESX server. The parameter is required when restoring a VMFS datastore, or a virtual machine that resides on a VMFS datastore, as well as when restoring an NFS virtual machine. The server name is the name of the ESX server as viewed through the vSphere Client. This name might differ from the host name or IP address of the ESX server.

[-backup-name {*backup name*}]

This optional parameter specifies which backup to restore. After adding the flag, you can add the name of the backup. If not specified, the latest available backup for the specified datastore or virtual machine is restored.

[-vmdk {*hard disk name*}]

This optional parameter specifies which hard disks are to be restored.

[-server {*server name*}]

This optional parameter specifies the name of the SnapManager for Virtual Infrastructure server to which you are sending this command. The default value is localhost.

[-restart-vm]

This optional parameter restarts the virtual machine after the restore operation.

[-quiet]

This optional parameter stops any output from displaying.

[-verbose]

This optional parameter provides detailed output when displaying information.

[-noprompt]

By default, a prompt appears, asking for confirmation when restoring a backup. This optional parameter disables the prompt.

[-user]

Add this optional parameter if you want to log in to the SnapManager for Virtual Infrastructure server with different credentials than you are currently logged in with.

[-help]

This optional parameter displays help for this command.

Example: Restoring a backup

The following example restores a virtual machine named nfs1-vm1 from a backup named backup-411:

```
smvi backup restore -id nfs1_vm1 -backup-name backup-411

Are you sure you want to proceed with this operation? [yes|NO] y
[11:04] Starting restore request
[11:04] [WARN] No active mounts found for datastore vmfs_ds1
(47ab69d8-e7c72da0-d6c5-001a6412251d)
[11:05] Restoring nfs virtual machine on folder 'nfs1_vm1'
[11:07] Reloading virtual machine
[11:07] Restore is complete
SMVICLI-0100: Command completed successfully
```

smvi backup unmount

The `smvi backup unmount` command unmounts a mounted virtual machine or datastore backup copy.

Syntax

```
smvi backup unmount -backup-name {backup name}    [-server {server
name}]    [-quiet]    [-verbose]    [-user]    [-help]
```

Description

Note: You must unmount a mounted backup copy to delete the backup copy or any of its preceding Snapshot copies.

Parameters

[-backup-name {*backup name*}]

This mandatory parameter specifies which backup copy to unmount. After adding the flag, add the name of the backup copy.

[-server {*server name*}]

This optional parameter specifies the name of the SnapManager for Virtual Infrastructure server to which you are sending this command. The default value is localhost.

[-quiet]

This optional parameter stops any output from displaying.

[-verbose]

This optional parameter provides detailed output when displaying information.

[-user]

Add this optional parameter if you want to log in to the SnapManager for Virtual Infrastructure server with different credentials than you are currently logged in with.

[-help]

This optional parameter displays help for this command.

Example: Unmounting a backup copy

The following example unmounts a backup copy named vmfs2_db:

```
smvi backup unmount -backup-name vmfs-2-db

[11:55] Starting unmount request
[11:55] Unmount is complete
SMVICLI-0100: Command completed successfully
```

smvi discover datastores

The `smvi discover datastores` command lists the datastores that are managed by the current vCenter Server and that reside on the storage systems currently assigned to your SnapManager for Virtual Infrastructure server.

Syntax

```
smvi discover datastores     [-help]
```

Parameters

`[-help]`

This optional parameter displays help for this command.

Example: Listing the datastores

The following example lists all the datastores managed by the current vCenter Server that reside on storage systems assigned to SnapManager for Virtual Infrastructure:

```
smvi discover datastores

Password for NETAPP\vanib: *********
Datacenter: Aladdin
Datastore: nfs_datastore6
NFS: 172.17.170.21:/vol/nfs_vol6
Datastore: nfs_datastore7
NFS: 172.17.170.21:/vol/nfs_vol7
Datastore: nfs_datastore7 (Backup test1)
NFS: 172.17.170.21:/vol/
nfs_vol7_mount_33e49878c5e74363825e84652a724aef
Datastore: nfs_datastore7 (Backup test0)
NFS: 172.17.170.21:/vol/
nfs_vol7_mount_90a6b1e7d6f948beaa6735af9692b3d4
Datastore: nfs_datastore7 (Backup backup_fgfdgfdgf_20080707134801)
NFS: 172.17.170.21:/vol/
nfs_vol7_mount_e50fc0eda0674cfbbf200f87f83ba8eb
Datastore: nfs_datastore8
NFS: 172.17.170.21:/vol/nfs_vol8
Datastore: nfs_datastore8 (Backup
backup_7d8597b0dfffd5c81806728dd45aea48)
NFS: 172.17.170.21:/vol/
nfs_vol8_mount_e7df47fbde00446cb6b589c821adc4dd
Datastore: vmfs_datastore5
LUN: 172.17.170.21:/vol/vmfs_vol5/lun5 Partition: 1
LUN: 172.17.170.21:/vol/vmfs_vol6/lun6 Partition: 1
Datastore: vmfs_datastore2
LUN: 172.17.170.21:/vol/vmfs_vol2/vmfs_lun2 Partition: 1
```

```
Datastore: vmfs_datastore3
LUN: 172.17.170.21:/vol/vmfs_vol3/lun3 Partition: 1
Datastore: vmfs_datastore4
LUN: 172.17.170.21:/vol/vmfs_vol4/lun4 Partition: 1
Datastore: vmfs_datastore7
LUN: 172.17.170.21:/vol/vmfs_vol7/qtree_vol7/lun7 Partition: 1
Datastore: snap-00000002-vmfs_datastore
LUN: 172.17.170.21:/vol/vmfs_vol1/vmfs_lun1 Partition: 1
Datastore: vmfs7_testAJ_1
LUN: 172.17.170.21:/vol/volaj1/lun1 Partition: 1
Datastore: vmfs7_testAJ-2
LUN: 172.17.170.21:/vol/volaj1/lun2 Partition: 1
Datacenter: Bellagio
```

smvi filerestore add-portgroup

The `smvi filerestore add-portgroup` command assigns virtual machines to a port group. You can also perform this operation using the VSC for VMware vSphere user interface.

Syntax

```
smvi filerestore add-portgroup [-name{port group name}] [-server{server
name}]     [-user] [-verbose]        [-help]
```

Parameters

[-name {*port group name*}]

This mandatory parameter specifies the name of the port group, or network, that is used to enable or disable administrator-assisted file-level restore operations.

[-server {*server name*}]

This optional parameter specifies the name of the SnapManager for Virtual Infrastructure server to which you are sending this command. The default value is localhost.

[-user]

Add this optional parameter if you want to log in to the SnapManager for Virtual Infrastructure server with different credentials than you are currently logged in with.

[-verbose]

This optional parameter provides detailed output when displaying information.

[-help]

This optional parameter displays help for this command.

smvi filerestore delete-portgroup

The `smvi filerestore delete-portgroup` command removes the port group and disables file restore sessions for the virtual machines assigned to the port group. You can also perform this operation using the VSC for VMware vSphere user interface.

Syntax

```
smvi filerestore delete-portgroup    [-name{port group name}]    [-server
{server name}]    [-user]    [-verbose]        [-help]
```

Parameters

[-name {*port group name*}]

This mandatory parameter specifies the name of the port group, or network, that is used to enable or disable administrator-assisted file-level restore operations.

[-server {*server name*}]

This optional parameter specifies the name of the SnapManager for Virtual Infrastructure server to which you are sending this command. The default value is localhost.

[-user]

Add this optional parameter if you want to log in to the SnapManager for Virtual Infrastructure server with different credentials than you are currently logged in with.

[-verbose]

This optional parameter provides detailed output when displaying information.

[-help]

This optional parameter displays help for this command.

smvi notification list

The `smvi notification list` command displays information about the alert notification.

Syntax

```
smvi notification list    [-server {server name}]    [-user] [-
verbose]    [-help]
```

Parameters

[-server {*server name*}]

This optional parameter specifies the name of the SnapManager for Virtual Infrastructure server to which you are sending this command. The default value is localhost.

[-user]

Add this optional parameter if you want to log in to the SnapManager for Virtual Infrastructure server with different credentials than you are currently logged in with.

[-verbose]

This optional parameter provides detailed output when displaying information.

[-help]

This optional parameter displays help for this command.

smvi notification set

The `smvi notification set` command displays information about the alert notification.

Syntax

```
smvi notification set    [-smtp server {dns name | ip address}]    [-from
{from email address}]    [-to {to email address}]        [-server
{server name}]    [-user] [-verbose]    [-help]
```

Parameters

[-smtp server {*dns name* | *ip address*}]

This mandatory parameter specifies the name or IP address of the SMTP server that handles the test notification e-mail.

[from {*from email address*}]

This mandatory parameter specifies the sender e-mail address.

[to {*to email address*}]

This mandatory parameter specifies the comma-separated list of recipient e-mail addresses.

[-server {*server name*}]

This optional parameter specifies the name of the SnapManager for Virtual Infrastructure server to which you are sending this command. The default value is localhost.

[-user]

Add this optional parameter if you want to log in to the SnapManager for Virtual Infrastructure server with different credentials than you are currently logged in with.

[-verbose]

This optional parameter provides detailed output when displaying information.

[-help]

This optional parameter displays help for this command.

smvi notification test

The `smvi notification test` command displays information about the test notification.

Syntax

```
smvi notification test    [-server {server name}]    [-user] [-
verbose]    [-help]
```

Parameters

[-server {*server name*}]

This optional parameter specifies the name of the SnapManager for Virtual Infrastructure server to which you are sending this command. The default value is localhost.

[-user]

Add this optional parameter if you want to log in to the SnapManager for Virtual Infrastructure server with different credentials than you are currently logged in with.

[-verbose]

This optional parameter provides detailed output when displaying information.

[-help]

This optional parameter displays help for this command.

smvi restoreagent set

The `smvi restoreagent set` command sets the default installation URL of the restore agent. You can also perform this operation using the VSC for VMware vSphere user interface.

Syntax

```
smvi restoreagent set    [-url]    [-server {server name}]    [-user]
[-verbose]    [-help]
```

Parameters

[-url]

This mandatory parameter provides an URL that points to a customer location for the restore agent installer.

[-server {*server name*}]

This optional parameter specifies the name of the SnapManager for Virtual Infrastructure server to which you are sending this command. The default value is localhost.

[-user]

Add this optional parameter if you want to log in to the SnapManager for Virtual Infrastructure server with different credentials than you are currently logged in with.

[-verbose]

This optional parameter provides detailed output when displaying information.

[-help]

This optional parameter displays help for this command.

smvi servercredential delete

The `smvi servercredential delete` command deletes a user account created by the `smvi servercredential set` command.

Syntax

```
smvi servercredential delete    -username {user name}    [-help]
```

Description

Note: You cannot run this command from a remote host.

Parameters

[-username {*user name*}]

This mandatory parameter specifies the internal user account that you want to delete.

[-help]

This optional parameter displays help for this command.

Example: Deleting a user account

The following example deletes the olduser2 user account:

```
smvi servercredential delete -username olduser2
SMVICLI-0100: Command completed successfully
```

smvi servercredential list

The `smvi servercredential list` command displays a user account created by the `smvi servercredential set` command.

Syntax

```
smvi servercredential list    [-help]
```

Description

Note: You cannot run this command from a remote host.

Parameters

[-help]

This optional parameter displays help for this command.

Example: Listing the server credentials

The following example lists the current SnapManager for Virtual Infrastructure server credentials:

```
smvi servercredential list

Username
-----------------------------------------------------------
administrator
```

smvi servercredential set

The `smvi servercredential set` command adds a user account for Backup and Recovery capability to use for authentication instead of your Windows user credentials.

Syntax

```
smvi servercredential set    [-help]
```

Description

Note: You cannot run this command from a remote host.

Parameters

`[-help]`

This optional parameter displays help for this command.

Example: Adding a user account

The following example adds a user account named administrator and sets a seven character password:

```
smvi servercredential set

Username: administrator
Password: *******
SMVICLI-0100: Command completed successfully
```

smvi storagesystem list

The `smvi storagesystem list` command lists the added NetApp storage systems.

Syntax

```
                smvi storagesystem list                [-server {server
name}]                [-user]                [-verbose]                [-
help]
```

Parameters

[-server {*server name*}]

This optional parameter specifies the name of the SnapManager for Virtual Infrastructure server to which you are sending this command. The default value is localhost.

[-user]

Add this optional parameter if you want to log in to the SnapManager for Virtual Infrastructure server with different credentials than you are currently logged in with.

[-verbose]

This optional parameter provides detailed output when displaying information.

[-help]

This optional parameter displays help for this command.

Example: Listing the storage systems

The following example lists the NetApp storage systems that reside in the local SnapManager for Virtual Infrastructure server; in this case, a single storage system with an IP address of 123.17.170.21:

```
smvi storagesystem list

Name                                IP Address
----------------------------------- --------------
123.17.170.21                       123.17.170.21
```

smvi version

The `smvi version` command displays the version of the VSC for VMware vSphere CLI and the SnapManager for VI server.

Syntax

```
smvi version    [-server {server name}]    [-help]
```

Parameters

[-server {*server name*}]

[-help]

This optional parameter displays help for this command.

Example: Displaying the version

The following example displays the VSC for VMware vSphere CLI and server version:

```
smvi version
SnapManager for Virtual Infrastructure CLI Rballys.4N_120127_0000
(Build: 120127
)
SnapManager for Virtual Infrastructure Server Rballys.
4N_120127_0000 (Build: 120
127)
```

Copyright information

Trademark information

NetApp, the NetApp logo, Network Appliance, the Network Appliance logo, Akorri, ApplianceWatch, ASUP, AutoSupport, BalancePoint, BalancePoint Predictor, Bycast, Campaign Express, ComplianceClock, Customer Fitness, Cryptainer, CryptoShred, CyberSnap, Data Center Fitness, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, DenseStak, Engenio, Engenio logo, E-Stack, ExpressPod, FAServer, FastStak, FilerView, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NearStore, NetCache, NOW (NetApp on the Web), Onaro, OnCommand, ONTAPI, OpenKey, PerformanceStak, RAID-DP, ReplicatorX, SANscreen, SANshare, SANtricity, SecureAdmin, SecureShare, Select, Service Builder, Shadow Tape, Simplicity, Simulate ONTAP, SnapCopy, Snap Creator, SnapDirector, SnapDrive, SnapFilter, SnapIntegrator, SnapLock, SnapManager, SnapMigrator, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapSuite, SnapValidator, SnapVault, StorageGRID, StoreVault, the StoreVault logo, SyncMirror, Tech OnTap, The evolution of storage, Topio, VelocityStak, vFiler, VFM, Virtual File Manager, VPolicy, WAFL, Web Filer, and XBB are trademarks or registered trademarks of NetApp, Inc. in the United States, other countries, or both.

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

Apple is a registered trademark and QuickTime is a trademark of Apple, Inc. in the United States and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the United States and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the United States and/or other countries.

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

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

NetApp, Inc. NetCache is certified RealSystem compatible.

How to send your comments

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us to provide the most accurate and high-quality information. If you have suggestions for improving this document, send us your comments by email to *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.

You can also contact us in the following ways:

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

Index

D

E

F

S

T

U

V

W

X

Z