Hitachi Storage (VASA) Provider for VMware vCenter

Virtual Storage Platform E series, F series, G series, 5000 series, VSP, HUS VM

v3.7.2

Deployment Guide

This manual provides information necessary to build an environment for the VMware vSphere APIs for Storage Awareness (VASA) provider for Hitachi Storage.

Contents

Contents

Contents

Contents

Preface

This deployment guide provides information to help your site implement VMware VASA features with Hitachi Virtual Storage Platform E series, F series, G series, 5000 series, VSP, and HUS VM.

Intended audience

This document is intended for:

- vSphere^{TM} system administrators
- Systems engineers

Readers of this document should be familiar with the basic operation of the following:

- Hitachi Virtual Storage Platform E series (VSP E series)
- Hitachi Virtual Storage Platform F series (VSP F series)
- Hitachi Virtual Storage Platform G series (VSP G series)
- Hitachi Virtual Storage Platform 5000 series (VSP 5000 series)
- Hitachi Virtual Storage Platform (VSP)
- Hitachi Virtual Storage Platform (HUS VM)
- VMware vSphere
- Oracle Linux

Product version

This document describes Hitachi Storage Provider for VMware vCenter (VASA Provider) Deployment v3.7.2.

Changes in this revision

The following are the major changes:

- A procedure was added for using Thin Image pairs for which the cascade attribute is enabled.
- A procedure was added for using the vCenter SSO group function.
- A procedure was added for expanding a backup disk.

Release notes

Read the release notes before installing and using this product. They may contain requirements or restrictions that are not fully described in this document or updates or corrections to this document. Release notes are available on the Hitachi Vantara Support Website: https://knowledge.hitachivantara.com/Documents.

Related documents for storage adapters and drivers are available at https://knowledge.hitachivantara.com/Documents/Adapters_and_Drivers/Storage_Adapters_and_Drivers.

Referenced documents

Hitachi documents:

- *Hitachi Storage (VASA) Provider for VMware vCenter vVols Replication Guide*, MK-92ADPTR153

- *Provisioning Guide for Open Systems*, MK-98RD9015

- *Provisioning Guide for Open Systems*, MK-92RD8014

- *Provisioning Guide*, MK-97HM85026

- *Provisioning Guide*, MK-94HM8014

- *System Administrator Guide*, MK-98RD9009

- *System Administrator Guide*, MK-92RD8016

- *System Administrator Guide*, MK-97HM85028

- *System Administrator Guide*, MK-94HM8016

- *Provisioning Guide or Virtual Storage Platform Provisioning Guide* , MK-90RD7022

Hitachi Vantara Support Connect, https://knowledge.hitachivantara.com/Documents

VMware documents:

- VMware vSphere ESXi

- VMware vSphere vCenter Server

Red Hat documents:

- Red Hat Enterprise Linux

Oracle documents:

- Oracle Linux

Document conventions

This document uses the following typographic conventions:

Convention	Description
Bold	- Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click **OK**. - Indicates emphasized words in list items.
Italic	- Indicates a document title or emphasized words in text. - Indicates a variable, which is a placeholder for actual text provided by the user or for output by the system. Example: `pairdisplay -g `*`group`* (For exceptions to this convention for variables, see the entry for angle brackets.)
`Monospace`	Indicates text that is displayed on screen or entered by the user. Example: `pairdisplay -g oradb`
< > angle brackets	Indicates variables in the following scenarios: - Variables are not clearly separated from the surrounding text or from other variables. Example: `Status-<`*`report-name`*`><`*`file-version`*`>.csv` - Variables in headings.
[ ] square brackets	Indicates optional values. Example: [a | b] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: { a | b } indicates that you must choose either a or b.
| vertical bar	Indicates that you have a choice between two or more options or arguments. Examples: [a | b] indicates that you can choose a, b, or nothing.

Convention	Description
	{ a | b } indicates that you must choose either a or b.

This document uses the following icons to draw attention to information:

Icon	Label	Description
	Note	Calls attention to additional information.
	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
	Important	Highlights information that is essential to the completion of a task.
	Caution	Warns the user of adverse conditions and/or consequences (for example, disruptive operations, data loss, or a system crash).
	CAUTION	Warns the user of a hazardous situation that, if not avoided, could result in major or minor injury.
	WARNING	Warns the user of a hazardous situation which, if not avoided, could result in death or serious injury.

Conventions for storage capacity values

Physical storage capacity values (for example, disk drive capacity) are calculated based on the following values:

Physical capacity unit	Value
1 kilobyte (KB)	1,000 (10^3) bytes
1 megabyte (MB)	1,000 KB or $1,000^2$ bytes
1 gigabyte (GB)	1,000 MB or $1,000^3$ bytes
1 terabyte (TB)	1,000 GB or $1,000^4$ bytes
1 petabyte (PB)	1,000 TB or $1,000^5$ bytes
1 exabyte (EB)	1,000 PB or $1,000^6$ bytes

Logical capacity values (for example, logical device capacity, cache memory capacity) are calculated based on the following values:

Logical capacity unit	Value
1 block	512 bytes
1 cylinder	Mainframe: 870 KB Open-systems: ▪ OPEN-V: 960 KB ▪ Others: 720 KB
1 KB	1,024 (2^{10}) bytes
1 MB	1,024 KB or $1,024^2$ bytes
1 GB	1,024 MB or $1,024^3$ bytes
1 TB	1,024 GB or $1,024^4$ bytes
1 PB	1,024 TB or $1,024^5$ bytes
1 EB	1,024 PB or $1,024^6$ bytes

Accessing product documentation

Product user documentation is available on the Hitachi Vantara Support Website: https://knowledge.hitachivantara.com/Documents. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Getting help

The Hitachi Vantara Support Website is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to the Hitachi Vantara Support Website for contact information: https://support.hitachivantara.com/en_us/contact-us.html.

Hitachi Vantara Community is a global online community for Hitachi Vantara customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hitachivantara.com, register, and complete your profile.

Comments

Please send comments to doc.comments@hitachivantara.com. Include the document title and number, including the revision level (for example, -07), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara LLC.

Thank you!

Chapter 1: Overview

Hitachi Storage Provider for VMware vCenter is a storage provider that allows you to use VASA features with supported Hitachi storage systems.

About the VASA Provider

Hitachi Storage Provider for VMware vCenter (VASA Provider) allows you to use the following VASA features with Hitachi storage systems.

In the policy-based datastore operation, you can create a datastore by selecting a Storage Container without any special knowledge of the storage system. You can create a virtual machine (VM) by setting policies (such as high IOPS and reliability) and can also verify whether the VM complies with these policies.

- VMware vSphere Virtual Volumes (vVols)

  Using VASA Provider allows vVols to be used with Hitachi storage systems.

- VMware Virtual Machine File System (VMFS)
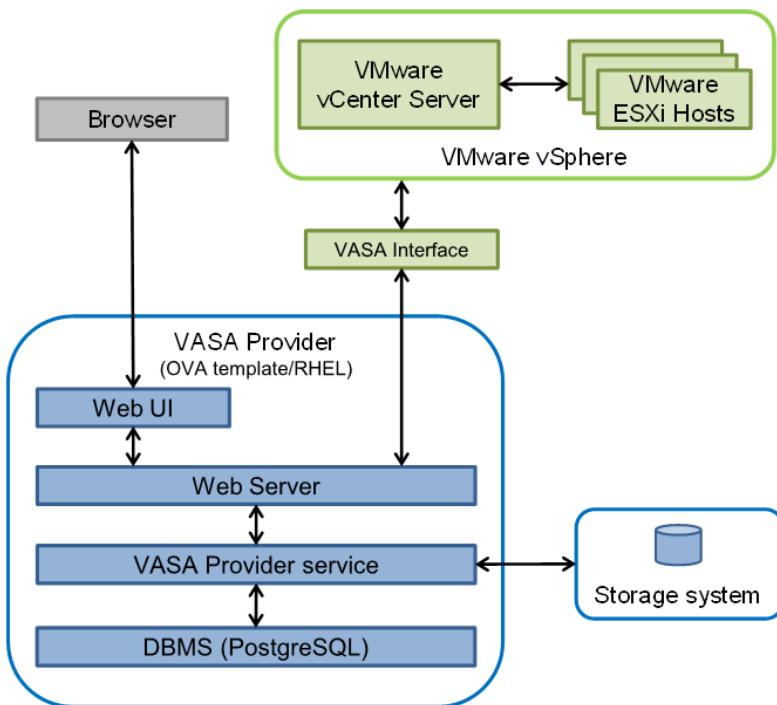
  - Storage Capability information and alert notifications related to VMFS filesystems are generated automatically and displayed in vCenter Server. For example, an alert will appear in vSphere Client when an LDEV's used capacity threshold is exceeded.

  - VMware SPBM tags for devices backing VMFS filesystems are provided, which associate the VMFS filesystems with storage profiles. These profiles allow storage policies to be configured in vSphere for VMFS filesystems in addition to VMware vVols. For example, in vCenter, a datastore can be assigned tags, such as "Encryption: Yes", which indicate various Capabilities.

See the VMware documentation for more VASA Provider information.

This manual explains the operation of vSphere Client by using the operation of vCenter Server 7.0 Update 3 as an example.

VASA Provider deployment architecture

The following diagram shows how the VASA Provider functions.

Key terms and concepts

Term	Description
ALU	Administrative Logical Unit An ALU is the volume that provides the access point to the virtual machine. To use a vVols, an ALU must be assigned to the ESXi host. ALU is called protocol endpoint in vSphere.
Block	Block storage refers to storage accessed using FC or iSCSI (instead of a NAS protocol like NFS).
PE	Protocol Endpoint A PE is a volume that serves as the access point. All I/O from ESXi to vVols pass through a PE. A PE is not intended to provide any capacity. A PE in a storage system is called an ALU.
SLU	Subsidiary Logical Unit An SLU is the destination volume where virtual machine data is stored. When a virtual machine is created, SLUs are created from a DP pool or Hitachi Thin Image pool and bound to an ALU (assigned a path). SLUs are called vVols on the virtual machine.

Term	Description
SPBM	Storage Policy-Based Management

SPBM is a mechanism that automatically decides where to create the vVols for a virtual machine from among the applicable storage resources. This decision is based on the virtual machine requirements defined by a virtual machine administrator. For example, if the required drive type for a virtual machine is SSD, VASA Provider searches for SSD DP pools and the volumes (vVols) created from the relevant DP pool are assigned to the virtual machine. |
Storage Container	A storage container is where resources such as DP pools and Hitachi Thin Image pools are collected for creating virtual machines, snapshots, and clones. DP pools and Hitachi Thin Image pools are added to resource groups and then made available to vSphere administrators by creating storage containers. There is a one-to-one relationship between a storage container and a resource group. DP pools are used to create virtual machines while DP pools or Hitachi Thin Image pools are used to create snapshots or clones. Storage containers are viewed from virtual machines as datastores.
VASA	Abbreviation for VMware vSphere APIs for Storage Awareness. This function indicates the overall storage management functions of vSphere.
VMFS	Abbreviation for VMware Virtual Machine File System. VMware Virtual Machine File System is a cluster file system developed by VMware. It enables you to use the storage area used by a system on a virtual machine and store disk images and snapshots of the virtual machine.
vVols	Abbreviation for VMware vSphere Virtual Volumes. VMware vSphere Virtual Volumes is the storage management technology implemented starting from VMware vSphere 6.0. Virtual disks of virtual machines are provided as disk volumes on the storage disk array. When you create a virtual machine, disks are created automatically, without requiring any operations on the storage system.

Chapter 1: Overview

Chapter 2: System requirements

The system requirements for the VASA Provider are as follows.

Hardware requirements

Component	Requirement
VSP (vVols not supported)	70-06 or later
HUS VM (vVols not supported)	73-03 or later
Virtual Storage Platform G1000	80-03 or later
VSP G200, G400, G600, G800	83-02 or later
VSP F400, F600, F800	83-02 or later
VSP G1500	80-05 or later
VSP G350, G370, G700, G900	88-07-01-x0/00 or later
VSP F350, F370, F700, F900	88-07-01-x0/00 or later
VSP F1500	80-05 or later
VSP 5100, 5500, 5100H, 5500H*	90-05-01-00/00 or later
VSP 5200, 5600, 5200H, 5600H*	90-08-01-00/00 or later
VSP E590, E790, E990, E590H, E790H	93-01-01-x0/00 or later
VSP E1090, E1090H	93-06-01-x0/00 or later
Host bus adapter	HBAs must support the **Secondary LUNID** feature to use vVols
Resource requirements for VMware to deploy the VASA Provider VM	- CPU: vCPU (4) - Main memory: 8 GB - HDD capacity: 200 GB - Ethernet: 1 Gbps or more is recommended

Component	Requirement
Display for Web UI of VASA Provider	▪ Display resolution: 1,600 x 900 or higher (recommended) ▪ Color depth: 24 bit or higher (recommended)
* You can create Thin Image pairs for which the cascade attribute is enabled. For more information, see Upgrading the VASA Provider (on page 26).	

Software requirements

Software	Requirements
VMware	▪ VMware vCenter Server 7.0/7.0 (Update 1/Update 2/Update 3) ▪ VMware ESXi 7.0/7.0 (Update 1/Update 2/Update 3) ▪ VMware vCenter Server 8.0 ▪ VMware ESXi 8.0
Multipath software	VMware NMP or Dynamic Link Manager (8.2.0-01 or later)
Browser	▪ Google Chrome ▪ Microsoft Edge ▪ Mozilla Firefox The supported versions are those that comply with the prerequisites for VMware vSphere Client.
VASA Provider	▪ PostgreSQL ▪ Oracle Linux 8.6 (This is the pre-installed guest operating system in this product's OVA file. If a problem occurs in Oracle Linux, contact Oracle Support. At this time, you might need to purchase support services from Oracle. If necessary, perform Oracle Linux security updates only. For information about installing security updates, see the documentation related to Oracle Linux.)
Storage Management Software (Optional)	▪ Hitachi Configuration Manager 8.6.0 and later (SVP or CM REST API Server is available for VASA Provider with VSP G350, G370, G700, G900 or VSP F350, F370, F700, F900. vVols is not supported for CM REST API Server.) ▪ Hitachi Ops Center Protector (Protector) 7.5.2 This is required if you want to use vVols Replication.

Chapter 2: System requirements

Software	Requirements
Virtual SVP	Virtual SVP is required when using VSP E590, E790, E990, E590H, E790H, E1090, E1090H storage system. Use a version corresponding to the SVOS version.

📄 **Note:** The VASA Provider supports vCenter Server Linked Mode. You must register it with each vCenter Server.

Supported protocols

The VASA Provider supports iSCSI and FC connections between ESXi hosts and storage systems.

Port and firewall requirements

Destination	Port number	Source
VASA Provider	▪ 50000/tcp ▪ 50001/tcp	vSphere Client, vCenter Server, ESXi, and Remote VASA Provider
vCenter Server (SDK), and Protector	443/tcp	VASA Provider
vCenter Single Sign-On (SSO) server	443/tcp	VASA Provider
SVP	▪ 1099/tcp ▪ 11099/tcp ▪ 51099/tcp ▪ 51100/tcp	VASA Provider

Restrictions and considerations for vVols Environments

Cancelling a Storage vMotion migration task or operation	Attempts to cancel a Storage vMotion task that is running might fail, but VM data will not be impacted.

Cancelling a VM snapshot creation task or operation	Do not cancel a snapshot task that is running. Cancellation might fail. Delete the snapshot data after the task finishes.
Cancelling a VM snapshot restore task or operation	Attempts to cancel a VM restore task that is running might fail. Retry the operation and make sure that it succeeds.
Expanding a volume after cloning	If expanding a volume results in an error shortly after cloning a VM in a vVols datastore, the cloning operation might still be running in the background. Wait a minute until the cloning operation finishes, and then try to expand the volume again.
File upload to vVols Datastore	VMware vSphere versions earlier than 8.0 do not support file upload to vVols datastores.
Managing LDEVs for which the SLU attribute is set	For LDEVs for which the SLU attribute is set, perform all VM and vVols operations by using vCenter. Do not directly access storage systems to change such LDEVs. Directly accessing storage systems to change the LDEVs might disrupt the VASA storage system configuration.
Modifying VM Storage Policy	For a storage container that has multiple pools and policies, you currently cannot move a VM and its vVols from one pool to another pool by modifying the VM storage policy. For more information, see *Cannot modify VM storage policy* in the online help.
Restarting the VASA Provider VM	If a storage system fails, the data (including VMs) in vVols datastores will be safe but might become inaccessible. After the storage system recovers or restarts, wait for the vVols datastores to show online status. If the problem persists, rescan VASA Provider. If you still cannot access the data, restart the VASA Provider VM. It might take some time for VASA Provider services to start and vVols datastores to become available.
SLU deletion	If you want to delete VMs after the operating system time has been changed, you might need to restart the VASA Provider VM. If you do not restart the VASA Provider VM, the SLUs (vVols) might remain on the storage system even after the VMs have been deleted.
Storage vMotion of VMs with hierarchical (branched) snapshots	Storage vMotion of VMs with hierarchical (branched) snapshots may fail, though the VM data residing at the Storage vMotion source will remain intact. It may be necessary to consolidate or remove a VM's hierarchical snapshots before using Storage vMotion.

VM disk format	For VMs managed by the VASA Provider, only VMs with VMware virtual disks using the VMware Thin Provision format are supported. If a VM has VMware virtual disks configured using either Thick Provision Lazy Zeroed or Thick Provision Eager Zeroed, the VM's data will still reside on the storage system using the VMware Thin Provision format.
LDEV ID for Mainframe	The LDEV ID for Mainframe is not supported. When including LDEV IDs for the mainframe, a storage system registration may fail.
Pool has different RAID level	Policy compliance checks will fail if the pool LDEVs have different RAID levels. When you create the VM storage policy, avoid using the Storage Capability of the RAID level.
Modifying storage policy for multiple vVols VMs	Policy compliance changes for vVols VMs can fail on the vCenter Server if a user applies them to multiple vVols VMs. It is recommended to change the policy compliance for each of the individual vVols VMs on the vCenter Server.
Refreshing storage system metadata in VASA	Changing the configuration of a storage system might cause attempts to refresh the storage system in VASA to fail. If the refresh operation fails, retry the operation.

Invalid VM name is displayed	When operations such as creating VMs and registering inventory are performed, an incorrect VM name might appear, as shown in the following example.
	
	`/vmfs/volumes/`
	`vvol:1a9f5bf045564e66-98d68378b6f26999/`
	`naa.60060E8130274C3`
	
	This might occur when a vCenter internal process is running. Wait for the process to complete, then refresh the vSphere Client screen to see if the VM name displays properly. If it does not, re-register the affected VM in the inventory, then verify if the VM name is displayed properly.

Web UI of the VASA Provider when certain symbols are used	If you use a backslash (\), single quote ('), or double quote (") in the vSphere environment, storage system, or data flow resources in Protector, the Web UI of the VASA Provider might not be displayed properly.
Virtual storage machines displayed in the Web UI of the VASA Provider	Virtual Storage on the Manage Storage Systems screen does not display the following virtual storage machines that are created on VSP F1500 and G1500: VSP F200, F400, F600, and F800 virtual storage machines and VSP G200, G400, G600, and G800 virtual storage machines.

User name and password for VASA Provider	The following characters cannot be used in the user name or password for VASA Provider: % & ' +
Preliminary work before migrating an ESXi host to another vVols environment	Before migrating an ESXi host used in one vVols environment to another vVols environment, perform the following operations. If you migrate the ESXi host without performing these operations, you might not be able to create or power on the VM in the environment to which it was migrated. ▪ On the ESXi host, delete the pre-migration vVols datastore. ▪ Unregister the ESXi host from the pre-migration vCenter Server.
Restriction on RAID Level in the Capability Profile	If Dynamic Tiering is enabled for a pool in a storage container, the value of RAID Level in the Capability Profile might be invalid and might not comply with the VM storage policy. If the pool satisfies both of the following conditions, do not use the RAID Level Capability. ▪ The pool has multiple volumes, and a different value is set for RAID Level for each volume. ▪ The pool volumes are external volumes.
Performing Data in Place upgrades	This version of VASA Provider does not support the use of Data in Place upgrades to migrate VSP storage systems to newer models.
vVols capacity	VASA Provider does not support the creation of vVols smaller than 48 MB.
Performing operations on a VM from which the linked clone of a linked clone VM is created	After a linked clone VM is created, revert operations from the VM snapshot from which the linked clone was created are not supported.
Linkage with backup software that supports VADP	When linking with and using backup software that supports VADP, the level of parallelism for obtaining backups must be no more than 8 parallels.

Changing the IP address (for vVols/VMFS)

▪ The VASA Provider must be configured with a static IP address; it doesn't support DHCP.

▪ Should it become necessary to change the VASA Provider's IP address, first change the IP address, then follow the steps below:

1. Renew the SSL certificate.

2. Restart the VASA Provider VM.

3. Re-register the VASA Provider in VMware vSphere.

Chapter 2: System requirements

Multiple VASA Providers (for vVols/VMFS)

- Supported configuration

  - The same VASA Provider is registered on multiple vCenter Servers.

  - There are multiple configurations in which one VASA Provider is registered on one vCenter Server, and the same storage system is registered in each VASA Provider.

    For example, VASA Provider A is registered on vCenter Server A, VASA Provider B is registered on vCenter Server B, and the same storage system is registered in both VASA Provider A and VASA Provider B.

- Unsupported configurations

  Multiple VASA Providers are registered on the same vCenter Server.

Notes on cloning virtual machines

- Attempts to clone multiple virtual machines at the same time sometimes fail. In such cases, try again.

- When cloning a virtual machine under a heavy load, an unused snapshot vmdk file might remain on the vCenter Server and the storage system. In such cases, clone the virtual volume and delete the old virtual machine. If a snapshot is remained in the storage system, delete the snapshot.

- If an attempt to clone multiple virtual machines at the same time sometimes fails, unused virtual volumes of Thin Image might remain on the resource group. In such cases, delete virtual volumes of Thin Image.

- If an attempt to clone a VM fails, a vVol (LDEV) might remain on the storage system. Perform the following procedure to check and delete the vVol.

  > ⚠ **Caution:** You cannot recover a vVol (LDEV) after it is deleted. Before deleting a vVol (LDEV), check the following to verify that the vVol (LDEV) is not being used.
  >
  > - Check whether the VMFS file name of the vVol you want to delete is the same as or includes the name of the VM for which cloning failed.
  >
  > - Check whether a vmx file or vmdk file that includes Make sure that the VMFS file name of the vVol you want to delete does not exists in a datastore in vSphere Client.

  1. Check the name of the VM for which cloning failed.
  2. In the Web UI of VASA Provider, select Manage Storage Containers. Next, select the storage container you are using, and then select the vVols tab.
  3. In the VMFS File column on the vVols tab, check whether the name of the VM for which cloning failed or an item that includes the name of that VM appears.
  4. If the relevant vVol exists, check the LDEV ID that appears in the Volume column.
  5. In Storage Navigator, delete the LDEV.
  6. In the Web UI of VASA Provider, refresh the information about storage system.

Chapter 2: System requirements

Notes on virtual machine snapshots

- Attempts to create snapshots when VASA Provider is under a heavy load sometimes fail. In such cases, try again.

- If the information about storage systems in VASA Provider is old, attempts to create snapshots sometimes fail. In such cases, in the Web UI of VASA Provider, refresh the information about storage systems, and then create the snapshot again.

- Attempts to revert snapshots of the multiple virtual machines at the same time sometimes fail. In such cases, try again.

- Adding a snapshot disk with Independent - Nonpersistent disk mode to the virtual machine is not supported.

Notes on when an error occurs during the operation of vSphere Client or VASA Provider:

If an error occurs during the operation of vSphere Client or VASA Provider and the error persists even after you restart the VASA Provider service, perform troubleshooting. If this does not resolve the error, perform the following procedure before contacting customer support. This procedure allows you to perform recovery of VASA Provider without losing VM data.

1. Confirm that the status of VASA Provider on the vSphere Client is Offline or Disconnected.

   If this condition is met, go to the next step.

2. Confirm that the following file ends with the parameter setting `vasaprovider.uid`.

   ```
   /usr/local/hitachivp-b/tomcat/webapps/VasaProvider/META-INF/
   VasaProvider.properties
   ```

   If this condition is met, go to the next step.

3. Deploy the same version of the VASA Provider VM with the same settings as the VASA Provider VM where the error occurred.

   The following are the template customization parameters to be specified during deployment.

   - `SSO Server Configuration`

   - `Network Configuration`

   - `System Configuration`

4. Use the SCP protocol or another method to transfer the following file located on the deployed VM. Replace the corrupt file on the original VASA Provider VM with this file.

   ```
   /usr/local/hitachivp-b/tomcat/webapps/VasaProvider/META-INF/
   VasaProvider.properties
   ```

Chapter 2: System requirements

5. Confirm that the permission of the transferred file is set to `-rw-r--r--` and the owner is set to `vptomcat`. If other values are set, set the permission to `-rw-r--r--` and the owner to `vptomcat`.

```
ls -l /usr/local/hitachivp-b/tomcat/webapps/VasaProvider/META-INF/ | grep
VasaProvider.properties
-rw-r--r-. 1 vptomcat vptomcat 15043 Nov 12 01:51 VasaProvider.properties
```

6. If you have changed the default setting for `Editable Setting values` in the file, change it back to the original default setting before the transfer. Create a backup file of `VasaProvider.properties` before changing the setting.

7. Restart the VASA Provider service; see Restarting the VASA Provider service (on page 64)

Chapter 3: Installing the VASA Provider

The procedure for installing the VASA Provider is as follows.

Installation overview

The VASA Provider is distributed as an OVA file and is deployed on VMware vSphere as a packaged virtual machine (VM) which includes the VASA Provider and all the dependencies.

Obtaining the VASA Provider

The VASA Provider OVA can be obtained from the following sources:

- The VASA Provider distribution media
- Download from Support Portal

Deploying the VASA Provider

Deploying the OVA creates a VM pre-installed with the VASA Provider and all of its prerequisites. Use these steps to deploy the OVA.

Then, perform the procedure described in <u>Verifying the installation (on page 29)</u> to start the deployed VM and log in to the Web UI.

Before you begin

- Confirm that a provisioned VMFS/NFS/vSAN datastore exists. The VASA Provider VM will reside on this datastore.
- Confirm that an FQDN or IP address of the ESXi host on which the OVA is to be deployed is correctly configured.
- If you are using a DNS server, confirm that reverse DNS lookup is available for the DNS server.

  To check whether reverse DNS lookup is available, specify an IP address for the `nslookup` command.

Procedure

1. Store the OVA file on the client operating system that uses vSphere Client.

> 📄 **Note:** You can browse files other than those stored on the client operating system. However, it might take time, because when you select a file, the file must be transferred over the network.

2. Deploy an OVF template. Select the VASA Provider OVA package, and then perform operations by following the on-screen instructions.

> 📄 **Note:** After deploying VASA Provider, configure `SSO Group` settings as needed. A function is available for managing user access permissions for SSO groups in vCenter. Note that this function is enabled by default. For details, see Logging in to the Web UI (on page 30).

Upgrading the VASA Provider

This section describes how to upgrade the OVA.

Upgrading the VASA Provider (from v3.7.0 or earlier to v3.7.2)

To upgrade the VASA Provider v3.7.0 or earlier to v3.7.2, perform the following procedure, and then see Upgrading the VASA Provider (from v3.7.2 or later) (on page 29) to upgrade to the latest version of VASA Provider.

Before you begin

- Upgrade the existing VASA Provider environment to v3.7.0.

  If you are upgrading from v3.7.0, you do not need to perform this step.

  For details, see *Hitachi Storage (VASA) Provider for VMware vCenter Deployment Guide* (MK-90ADPTR010-30).

- As a precaution against problems that might occur during the upgrade, take a VM snapshot of VASA Provider.

- Make sure there are no tasks that are still running.

- In an environment where vVols Replication is used, upgrade the vVols Replication environment before upgrading the VASA Provider. For details, see the procedure for upgrading the vVols Replication environment in the *Hitachi Storage (VASA) Provider for VMware vCenter vVols Replication Guide*.

- If you are using a storage model that supports Thin Image pairs for which the cascade attribute is enabled (for details, see Hardware requirements (on page 16)), you need to select whether to use Thin Image pairs for which the cascade attribute is enabled or Thin Image pairs for which the cascade attribute is disabled.

  - If you use Thin Image pairs for which the cascade attribute is enabled (this setting is recommended and enabled by default), you will need to perform the following procedure before the upgrade. For details about Thin Image pairs for which the cascade attribute is enabled, see the manuals for the storage system.

    1. Make sure there are no snapshots for virtual machines on storage system models that support Thin Image pairs for which the cascade attribute is enabled.

    2. If such snapshots exist, delete them. For details on how to check and delete snapshots, see the documentation provided by VMware.

    > **Note:** By using Thin Image pairs for which the cascade attribute is enabled, you can then use the following functions:
    >
    > - Support for Fast Clone vVols
    >
    >   You can use Independent - Nonpersistent disk mode. This mode is mainly used in backup software that uses VADP when adding snapshots to virtual machines as hard disks.
    >
    > - Support for the cascade attribute and the clone attribute for Thin Image pairs
    >
    >   During the cloning of virtual machines that are powered on, the data in those virtual machines is copied by using storage systems, thereby reducing the load on servers.

  - If you want to use Thin Image pairs for which the cascade attribute is disabled because, for example, you do not want to erase snapshots of existing VMs, perform the following upgrade procedure to change the value of `server.cascade.snapshot.enable` to `false` in the `vvoladapter.properties` file.

Procedure

1. Unregister the old version of VASA Provider from VMware vSphere. See Removing the VASA Provider from vCenter Server (on page 38).

2. Log in as root to the guest OS of the old VASA Provider VM.

3. Stop the VASA Provider.

   ```
   # /etc/init.d/tomcat_vp_b stop
   ```

4. Export the data with the following command:

   ```
   # pg_dumpall -c -p 50003 -U postgres -f pg_dumpall_vpdata.sql
   ```

5. Save the exported data to another server or some other location.

6. Power off the VASA Provider virtual machine.

7. Deploy the new version of VASA Provider as a separate VM, and power it on. After deployment, log in to the Web UI. For details, see Deploying the VASA Provider (on page 25).

8. Copy the exported data (`pg_dumpall_vpdata.sql`) to the guest OS of the new VASA Provider VM.

9. Log in as root to the guest OS of the new VASA Provider VM.

10. Stop the VASA Provider.

    ```
    # /usr/local/hitachivp-b/tomcat_vp_b stop
    ```

11. Import the data with the following command:

    ```
    # psql -f pg_dumpall_vpdata.sql -U postgres -p 50003
    ```

12. If you use Thin Image pairs for which the cascade attribute is disabled, perform the following operation.

    a. Log in to the guest operating system of the VASA Provider VM as the root user (root/password).

    b. Open the `vvoladapter.properties` file in a text editor. For `server.cascade.snapshot.enable`, set the value `false`. The `vvoladapter.properties` file is located in the following directory:

       ```
       /usr/local/hitachivp-b/tomcat/webapps/VasaProvider/META-INF
       ```

13. Start the VASA Provider.

    ```
    # /usr/local/hitachivp-b/tomcat_vp_b start
    ```

14. A function is available for managing user access permissions for SSO groups in vCenter. Note that this function is enabled by default.

    - If you want to use the function for managing user access permissions for SSO groups in vCenter:

      Make sure that the vCenter SSO accounts and groups meet the requirements.

      To use a vCenter SSO group other than the default group, set the vCenter SSO group name in the `VasaProvider.properties` file.

      For details, see Logging in to the Web UI (on page 30).

    - If you do not want to use the function for managing user access permissions for SSO groups in vCenter:

      Set the value of `sso.user.group.check` to `false` in the `VasaProvider.properties` file.

      For details, see Logging in to the Web UI (on page 30).

15. Register the new VASA Provider. See Registering the VASA Provider in vCenter Server (on page 37).

Upgrading the VASA Provider (from v3.7.2 or later)

Use the VASA Provider Web UI to update the VASA Provider software or the Web UI software as needed.

> **Note:**
>
> - To prepare for the possibility that a problem might occur during the upgrade, a good practice is to acquire a database dump before performing the upgrade. For details about how to acquire a database dump, see VASA Provider migration (on page 61).
>
> - Clearing the cache might be necessary when the display is not updated.
>
> - If the upgrade fails and the VASA Provider stops working, please contact customer support.

Before you begin

This procedure only applies to VASA Provider versions v3.7.2 or later.

> **Note:** Proceed only when there are no running tasks.

The software file name resembles `file_name_xxx_update_patch.tar.gz`.

Verify the version number.

Procedure

1. To remove the VASA Provider, see Removing the VASA Provider from vCenter Server (on page 38).
2. Select the **Update Software** option.
3. Click **Choose File**, and then browse to the software to update.
4. Select the `.tar.gz` file.
   a. Browse to the location where you want to upload the file.
   b. Transfer the file to the VASA Provider.

   > **Important:** Do not close or refresh your browser during the data transfer.

   c. After the upload is complete, click **Apply**.

5. To register the VASA Provider, see Registering the VASA Provider in vCenter Server (on page 37).
6. Refresh storage information by using the procedure in Refreshing storage system information (on page 46).

Verifying the installation

This section explains how to verify that VASA Provider was successfully installed.

Starting the VM

After successful OVA deployment, a newly deployed VM is automatically created based on the configuration you provided during the deployment process.

> ❗ **Important:** You must start the newly deployed VM before you can log in.

Procedure

1. In vSphere Client, select the VM and power it on.

Logging in to the Web UI

After installing the VASA Provider, start a browser and enter the URL of the VASA Provider to verify that you can log in.

Before you begin

- A function is available for managing user access permissions for SSO groups in vCenter. You can configure settings so that only users belonging to the specified SSO group can perform actions such as registering VASA Provider in vCenter Server and logging in to VASA Provider. When you use this function, make sure that the following conditions are met.

  - The vCenter SSO account and the group meet the following conditions:

    - The vCenter SSO account and the group belong to the vSphere domain. (Default: vsphere.local)

    - The account name and group name are each no more than 255 characters long, and the password is in the range from 8 to 20 characters long. The account name, password, and group name use the following characters.

      For the account name:

      ```
      A-Z a-z 0-9 ! # $ { } * - . = | / ?
      ```

      For the group name:

      ```
      A-Z a-z 0-9 ! # $ % & ' { } * + - . = ^ | ~ / ? `
      ```

      For the password:

      ```
      A-Z a-z 0-9 ! # $ { } * - . = @ ^ | ~ / ? ` \
      ```

    If these conditions are not met, create a vCenter SSO account and a group that meet the conditions. For details on how to create these, see the documentation provided by VMware.

  - The roles and global permissions assigned to the vCenter SSO account are as follows.

    - The roles have been assigned **Modify permission** in the **Permissions** category. **Modify permission** is an additional permission that is needed to manage user access permissions for SSO groups in vCenter.

    - When global permissions were assigned, the **Propagate to children** check box was selected.

    For details on how to assign roles and Global Permissions, see the documentation provided by VMware.

  - The vCenter SSO group is specified for `sso.group` in `VasaProvider.properties`. (Default: `Administrators`) To use a vCenter SSO group other than the default, perform the following procedure to specify the group.

    1. Log in to the guest operating system of the VASA Provider VM as the root user (root/password).

    2. Open the `VasaProvider.properties` file in a text editor. Set the value of `sso.group` to the vCenter SSO group name. You cannot specify multiple vCenter SSO group names. The `VasaProvider.properties` file is located in the following directory:

```
/usr/local/hitachivp-b/tomcat/webapps/VasaProvider/META-INF
```

3. Restart the VASA Provider service. For details, see <u>Restarting the VASA Provider service (on page 64)</u>.

- The vCenter SSO account is a member directly under the vCenter SSO group. For details on how to add a member to the vCenter SSO group, see the documentation provided by VMware.

> **Note:**
>
> If you do not use this function, perform the following procedure.
>
> 1. Log in to the guest operating system of the VASA Provider VM as the root user (root/password).
>
> 2. Open the `VasaProvider.properties` file in a text editor. Change the value of `sso.user.group.check` to `false`. The `VasaProvider.properties` file is located in the following directory:
>
>    ```
>    /usr/local/hitachivp-b/tomcat/webapps/VasaProvider/META-INF
>    ```
>
> 3. Restart the VASA Provider service. For details, see <u>Restarting the VASA Provider service (on page 64)</u>.

- When you use SPBM tag, Tagging Admin must be available in the vCenter SSO account.

Procedure

1. Enter the VASA Provider URL in your browser:
   ```
   https://VASA-Provider-IP-Address:50001/
   ```

2. In the Web UI window, enter the **vCenter SSO** account and **password** (or **system** and **manager**) and click **Login**.
   The VASA Provider information is displayed on the Web UI's main window.

Item	Description
Service Name	Service name of the VASA Provider
Service Version	VASA Provider version
VASA Version	VASA API version
Supported Model	A list of supported storage system models

> **Note:** You must synchronize the vCenter Server, ESXi, and the VASA Provider to the same NTP server. If they are not synchronized to the same NTP server, you cannot register VASA Provider in vCenter Server. It is recommend that you configure the NTP server during OVA deployment.

Chapter 4: Configuring the VASA Provider

The following explains the settings required to use the VASA Provider.

Overview of VASA Provider settings

After deploying the VASA Provider, register storage systems in VASA Provider and register VASA Provider in VMware vSphere by performing the procedures in the following sections. If you want to use vVols, create storage containers for the vVols and perform other operations by following the procedure in Required setup for vVols environments (on page 33). If you want to use VMFS, configure the storage policy settings for VMFS and perform other operations by following the procedure in Required setup for VMFS environments (on page 40).

Common settings (set host groups)

To make LDEVs available to ESXi hosts, storage system host groups must be configured. See Referenced documents for more information about storage system configuration.

VAAI must be configured for both traditional VMFS and vVols datastores.

To enable VAAI, set the host mode of the host group to 21 (VMware Extension) and ensure that the following Host Mode Options are enabled for the host group:

- 63
- 114

Required setup for vVols environments

This section introduces the required setup for vVols environments.

Overview of the required settings for a vVols environment

The required tasks and setting locations for configuring vVols environments are listed in the table below.

Task	Setting location
Configuring the protocol endpoint (ALU) (on page 34)	Storage system
Configuring storage system resources and resource groups (on page 34)	Storage system
Registering storage systems (on page 37)	VASA Provider
Setting up a storage container (on page 37)	VASA Provider
Registering the VASA Provider in vCenter Server (on page 37)	vSphere Client
Creating a vVols datastore (on page 39)	vSphere Client
Managing Storage Policy Based Management (on page 39)	vSphere Client

Configuring the protocol endpoint (ALU)

The protocol endpoint (a vVols term) is a storage volume that serves as the access point. On the storage system, the protocol endpoint is known as the assigned logical unit, or ALU. A protocol endpoint (ALU) must be assigned to an ESXi host in order to use vVols. Creating protocol endpoints and assigning them to a VMware ESXi host are done using Device Manager - Storage Navigator.

> **Note:**
>
> - If you modify the protocol endpoint (ALU) or host group settings on the storage system, you must also update the VASA Provider's storage system information.
>
> - If you use an FC switch, we recommend that you specify single-initiator zoning or single-initiator-single-target zoning for the zoning setting.

Configuring storage system resources and resource groups

You must configure the required storage system resources and resource groups before you can use vVols.

vVols use DP pools to store virtual machine data, and they use Hitachi Thin Image pools to store snapshot data. A vVols virtual machine configuration file uses multiple LDEV IDs in order to configure a 1:1 correspondence with the LUNs. By creating a resource group on a storage system, you can consolidate resources such as pools and LDEV IDs. vVols can also use meta resources on the storage system.

There is a one-to-one correspondence between a resource group on the storage system and a VASA Provider storage container. When you create a virtual machine, use the resource group as the vVols datastore.

Chapter 4: Configuring the VASA Provider

Use Device Manager - Storage Navigator to create DP pools, Hitachi Thin Image pools, and resource groups, and to set up LDEV IDs. For details about these operations, see the documentation listed in Referenced documents (on page 8).

> 📄 **Note:** To make snapshots available with DP pools only and without creating Hitachi Thin Image pools, make sure that the following conditions are met.
>
> ▪ The storage systems are of the following models.
>
>   • VSP E series
>
>   • VSP G1000, VSP G1500 and VSP F1500 (microcode version 80-05-44-00 and later)
>
>   • VSP Gx00 and VSP Fx00
>
>   • VSP 5000 series
>
> ▪ The user does not use Dynamic Tiering in vVols.
>
> Use Hitachi Thin Image pools if they are already created.

For resources used by vVols, please check the following:

▪ If you modify a resource or resource group on the storage system, try Refreshing storage system information (on page 46).

▪ When expanding the capacity of a Hitachi Thin Image pool, do not operate VMs using the pool until the expansion is finished.

▪ Set an LDEV ID that can be used as an SLU in a resource group.

▪ Pay particular attention to the number of LDEV IDs if you manage VMFS datastore LDEVs in a resource group used by vVols.

▪ If you must move a vVols VM, do not move it directly on the storage system; use vMotion instead.

▪ When using multiple VASA Providers, do not share resource groups among them.

> ⚠️ **Caution:**
>
> ▪ Provide enough capacity for the DP pool and Hitachi Thin Image pool. If the capacity is insufficient, VMs might fail to operate. It is recommended that you set the capacity alert threshold for the pool.
>
> ▪ Ensure that there are enough unused LDEV IDs, because you will need LDEV IDs to create SLUs. If there are not enough unused LDEV IDs, VMs might fail to operate.
>
> ▪ While using a virtual machine, do not delete the relevant storage resources. If you delete the resources, the VM might stop running. The storage resources include the resource group containing its SLUs (vVols), the LDEV IDs being used by its SLUs, and the DP pool used to store its SLUs.

The table below shows an example of how to register a resource group for use with a vVols.

Use	Resource	Description
DP Pool	LDEV ID	Register the desired DP pool volume.
Hitachi Thin Image Pool	LDEV ID	Register the desired Hitachi Thin Image pool volume.
SLU	LDEV ID	Register LDEV IDs for SLU assignments. For vVols, use multiple LDEV IDs per VM. See the following table to verify the number of required LDEV IDs that must be registered.
DP Pool (reserve)	LDEV ID	vVols can utilize multiple DP Pools, if necessary. When creating storage containers, create a Capability Profile for each DP Pool to be used for specific purposes.

The table below shows the number of LDEV IDs used per vVols VM.

LDEV ID use	Number required
Configuration management (Config)	1
Data	Number of VM hard disks
VM startup (Swap)	1
VM snapshot (with memory) acquisition (Memory)	Number of VM memory snapshot acquisitions
VM suspension (Memory)	1

Linking with Dynamic Tiering and active flash

If VASA Provider is linked with Dynamic Tiering or active flash, vVols (SLUs) are automatically stored in the appropriate tiers based on the user-specified Storage Capabilities.

To use this function, enable Dynamic Tiering or active flash for the pools to be registered in the resource group. In addition, configure tiers and set the default schedule according to the storage configuration to be used.

For information about operating procedures when this function is enabled, see Using vVols Policy Compliance (on page 40). For information about how to specify settings for Dynamic Tiering and active flash, see the manuals for the storage system.

How to add a DP/Hitachi Thin Image pool to a resource group

LDEV IDs represent DP pools and Hitachi Thin Image pools on the Resource Group screen in Storage Navigator. Therefore, when adding a DP pool or Hitachi Thin Image pool to a resource group, add it by selecting an LDEV ID corresponding to an LDEV in the intended pool. This will automatically add all other LDEV IDs associated with the same pool to the resource group.

Procedure

1. For **Administration** in **Explorer**, select **Resource Groups**, and then click **Create Resource Groups**.
2. In the **Create Resource Groups** dialog box, click **LDEV Selection**.
3. In the **Pool Name (ID)** column in the **LDEV Selection** dialog box, look for an LDEV ID that is associated with the relevant pool.
4. Select an LDEV ID, and then click **Add**.

Registering storage systems

Storage systems used for vVols should be registered with the VASA Provider. See Managing storage systems (on page 45).

Setting up a storage container

Each vVol storage container corresponds to a storage system resource group (containing both DP pools and Hitachi Thin Image pools and LDEV IDs).

To use vVols, you must create a storage container corresponding to the storage system's resource group, and set Capability Profiles for each DP pool in the storage container. See Managing storage containers (for vVols) (on page 47).

Registering and removing the VASA Provider in vCenter Server

Registering the VASA Provider in vCenter Server

Use vSphere Client to register the VASA Provider with vCenter Server.

> **Note:** If you cannot register the VASA provider with vCenter Server, the certificate may have expired. Verify the expiration date of the vCenter Server certificate.

Procedure

1. Log in to vSphere Client, and then navigate to vCenter Server.
2. In the right pane, select the **Configure** tab, and then click **Storage Providers**.
3. Click **Add** to register a new storage provider.
4. In the **New Storage Provider** dialog, enter values for the fields shown below.

Item	Description
Name	Any name (example: VASA Provider)

URL	The VASA Provider URL
	
	`https://VASA-Provider-IP-Address-or-FQDN:50001/`
	`version.xml`

User name	vCenter SSO account name `(example: vsphere.local\Administrator)` For information on the types and number of characters that can be used for a vCenter SSO account name and on the requirements for using the function for managing user access permissions for SSO groups in vCenter, see Logging in to the Web UI (on page 30).
Password	vCenter SSO Password For information on the types and number of characters that can be used for a vCenter SSO password and on the requirements for using the function for managing user access permissions for SSO groups in vCenter, see Logging in to the Web UI (on page 30).

5. Click **OK**. If a **Security Alert** window appears, click **Yes**.

> 📄 **Note:** When the VASA Provider is registered for the first time, the following error is displayed by VMware vSphere:
>
> ```
> A problem was encountered while registering the provider. The
> certificate is not trusted.
> ```
>
> If the VASA Provider registration completes and goes online, the message can be ignored.

6. Confirm that the registration was successful by viewing the following:

   ▪ The **Storage Providers** section in the vSphere Client displays the newly added VASA Provider.

   ▪ The VASA Provider displays the registered storage system name.

Next steps

Proceed to Creating a vVols datastore (on page 39).

Removing the VASA Provider from vCenter Server

Use vSphere Client to remove the VASA Provider from vCenter Server.

Procedure

1. Log in to vSphere Client, and then navigate to vCenter Server .

2. In the right pane, select the **Configure** tab, and then click **Storage Providers**.

3. Select the VASA Provider to be removed and then click **Remove**.

4. In the confirmation window, click **Yes**.

Creating a vVols datastore

After you have successfully registered the VASA Provider, you can create a vVols datastore.

Before you begin

A storage container has been created by the VASA Provider.

Procedure

1. Log in to vSphere Client, and then go to **Host and Clusters**.

2. In the pane on the left, select the data center for which you want to create the vVols datastore.

3. In the pane on the right, select **Actions**, and then click **Storage** > **New Datastore**.

4. In the **Type** screen, select **vVol** and then click **NEXT**.

5. On the **Name and container selection** screen, enter the name of the datastore to be created in **Name**, select the storage container you want to use from the storage containers listed in **Backing Storage Container**, and then click **NEXT**.

6. In the **Select hosts accessibility** screen, select the check boxes to add the hosts that you want to associate with your datastore, and then click **NEXT**.

7. In the **Ready to complete** screen, review your settings, and then click **FINISH**.
   The new vVols datastore now appears under your data center in the pane on the left.

Managing Storage Policy Based Management

One of the prerequisites for configuring a VMware vVols environment requires you to define Storage Policy Based Management (SPBM). SPBM is a structure defined by a VM storage policy.

A Capability Profile defines Capabilities of a storage container (for example, IOPS, Latency, Availability). The VM administrator can check both the storage container and its associated Capability Profile.

The following steps outline the general task workflow for creating an SPBM structure.

Procedure

1. Define the Capability Profile according to <u>Creating a storage container (on page 47)</u>.

2. Create a VM storage policy in vCenter Server.

   Include the Storage Capability that you specified when you created the Capability Profile in the VM storage policy.

3. Check for compliance with the storage policy.

   vCenter reports whether storage containers exist that meet the policy criteria. This is done by comparing the Capability Profiles and VM storage policies.

4. Assign the created storage policy and create a VM.

Using vVols Policy Compliance

If vVols Policy Compliance is enabled, vVols (SLUs) are automatically stored in the appropriate tiers based on the user-specified Storage Capabilities.

Perform this procedure as needed.

Before you begin

- vVols datastores that include pools for which Dynamic Tiering or active flash is enabled have been created.

- vVols Policy Compliance is enabled.

Procedure

1. Create a Capability Profile.

   For details about the procedure, see Creating a storage container (on page 47).

   To check the correspondence between Storage Capabilities and the tiers in which datastores are stored, check **VM Policy** in the table for the **Enable vVol Policy Compliance** check box on the **Capability Schema** screen.

   For details about the procedure, see Enabling vVols Policy Compliance (on page 52).

2. Create a VM storage policy in vCenter Server.

   In the VM storage policy, include the Storage Capabilities you specified when you created the Capability Profile.

3. Assign the created VM storage policy to a VM.

   > 📄 **Note:** This function is used only when you change a VM storage policy. To create or clone a VM or to execute vMotion for a VM, select the default policy, and then change the VM storage policy.

Required setup for VMFS environments

This section explains how to use the VASA Provider in VMFS environments.

Overview of the required settings for a VMFS environment

The required tasks and setting locations for configuring VMFS environments are listed in the table below.

Task	Setting location
Configuring storage system resources and LDEVs (on page 41)	Storage system
Create VMFS datastores (on page 41)	vSphere Client

Task	Setting location
Registering storage systems (on page 41)	VASA Provider
Creating Tag-based Storage Policy configurations (on page 41)	VASA Provider
Registering the VASA Provider in vCenter Server (on page 37)	vSphere Client
Creating a Storage Policy Based Management (SPBM) for VMFS datastores (on page 42)	vSphere Client

Configuring storage system resources and LDEVs

LDEVs for VMFS datastores must be created on the storage system. The VASA Provider only supports DP pool LDEVs (virtual volumes); therefore, prepare the DP pool before creating the LDEVs.

See Referenced documents for more information about storage system configuration.

Linking with Dynamic Tiering and active flash

If VASA Provider is linked with Dynamic Tiering and active flash, VMFS datastores are automatically stored in the appropriate tiers based on the user-specified Storage Capabilities.

To use this function, enable Dynamic Tiering or active flash for the pools to be registered in the resource group. In addition, configure tiers and set the default schedule according to the storage configuration to be used.

For information about operating procedures when this function is enabled, see Using VMFS Policy Compliance (on page 43). For information about how to specify settings for Dynamic Tiering and active flash, see the manuals for the storage system.

Create VMFS datastores

To create VMFS datastores, see documentation provided by VMware Inc.

Registering storage systems

Storage systems to be used with VMFS must be registered with VASA Provider. See Managing storage systems (on page 45).

Creating Tag-based Storage Policy configurations

For VMFS datastores, you can configure a Tag-based Storage Policy.

The functions provided are the same as those that Storage Policy Based Management (SPBM) provides for vVols.

Chapter 4: Configuring the VASA Provider

Procedure

1. Refer to <u>Accessing the Manage Volumes screen (on page 49)</u>, and open the **Manage Volumes** screen.

2. Select an LDEV, then click **Define Profile**.

3. Click **Submit** after setting the Capability Profile (Profile Tag). To see a list of available Capability Profile values, click **Capability Schema**.

   ▪ Storage profiles reside in the same vCenter Server instance used by the VASA Provider for SSO authentication.

   ▪ It may take up to five minutes for the Tag-based Storage Policy to be reflected in vCenter Server.

   ▪ The storage profile is set for each pool after a storage container is created. The profile will be applied to all datastore LUNs in the pool being used.

   > 📄 **Note:** After a Capability Profile is configured in the VASA Provider, the LDEV's Capabilities will appear in vCenter Server as tags. To use SPBM in this environment, configure VM Storage Profile settings with these tags.

   Related references

   ▪ For creating a storage profile, see <u>Creating an LDEV storage profile (on page 49)</u>.

   ▪ For setting SPBM, see <u>Managing Storage Policy Based Management (on page 39)</u>.

   ▪ For registering the VASA Provider, see <u>Registering the VASA Provider in vCenter Server (on page 37)</u>.

Creating a Storage Policy Based Management (SPBM) for VMFS datastores

SPBM is a structure defined by a VM storage policy.

One of the prerequisites for configuring a VMFS environment involves configuring Storage Policy Based Management (SPBM).

Procedure

1. Log in to vSphere Client.

2. From the menu in the upper left of the screen, select **Policies and Profiles**.

3. On the **Policies and Profiles** screen, select **VM Storage Policies**.

4. On the **VM Storage Policies** screen, click **CREATE**.

5. On the **Name and description** screen, enter a name in **Name:** and then click **NEXT**.

   The **Policy structure** screen appears.

6. On the **Policy structure** screen, select the **Enable tag based placement rules** check box for **Datastore specific rules** and then click **NEXT**.

   The **Tag based placement** screen appears.

7. On the **Tag based placement** screen, perform the following steps:

   a. Select **SPBM** for **Tag category**.

b. Click **BROWSE TAGS** for **Tags**.

The **Add tags** screen appears.

8. On the **Add tags** screen, select the check box of the tag you want to add and then click **OK**.

9. On the **Tag based placement** screen, confirm the tag you added and then click **NEXT**.

10. On the **Storage compatibility** screen, confirm that a datastore compatible with the tag you added in step 8 is displayed and then click **NEXT**.

11. On the **Review and finish** screen, confirm the settings and then click **FINISH**.

12. On the **VM Storage Policies** screen, confirm that the created policy has been added to the list.

If you select a policy and then select **Storage Compatibility**, a datastore compatible with the tag you added in step 8 will be displayed as in step 10.

Using VMFS Policy Compliance

If you enable VMFS Policy Compliance, VMFS datastores are automatically stored in the appropriate tiers based on the user-specified Storage Capabilities.

Perform this procedure as needed.

Before you begin

- Datastores have been created from LDEVs in pools for which Dynamic Tiering or active flash is enabled.

- VMFS Policy Compliance is enabled.

Procedure

1. Create a Capability Profile.

   For details about the procedure, see Creating an LDEV storage profile (on page 49).

   To check the correspondence between Storage Capabilities and the tiers in which datastores are stored, check **VM Policy** in the table for the **Enable VMFS Policy Compliance** check box on the **Capability Schema** screen.

   For details about the procedure, see Enabling VMFS Policy Compliance (on page 53).

   📄 **Note:** This function is intended for datastores. Even if you change the VM storage policy in vCenter Server, this function will not be used.

Chapter 5: Using the VASA Provider

The VASA Provider provides the following functions, which can be accessed by using the web UI.

List of VASA Provider settings configurable from the Web UI

You can use the Web UI to configure the VASA Provider settings described in the following table.

Operation	Function	Description
Management[1]	Manage Storage Systems	Add, remove, refresh, edit, or display storage systems. Display or configure VMFS datastore LDEVs.
	Manage Storage Containers	Create, delete, edit, or display storage containers.
	Capability Schema	Display available Storage Capability values.
	Replication Groups	Create, delete, or display replication groups.
Maintenance[2]	General Settings	Register or update vCenter Single Sign-On (SSO) information. Register or delete the VASA Provider at the remote site. Register or delete a Protector Master.
	Download Logs	Download log files generated by the VASA Provider.
	Update Certificate	Update the SSL certificate file for vCenter Server.
	Change Credentials	Change the user name and password of the administrator account. The default user name is `system`, and the default password is `manager`.
	Restart Service	Restart the VASA Provider service.

Operation	Function	Description
	Resolve and Troubleshoot	Display the Logs and Troubleshooting Guide. If you display the log but do not find any error codes, the log file might have wrapped around. In this case, check the logs acquired by running Download Logs.
	Update Software	Update the VASA Provider.

Notes:

1. To perform this operation, log in using a vCenter SSO account.
2. To perform this operation, log in using a vCenter SSO account or the administrator account (default: `system`).

For details about the VASA Provider and its various functions, see the manuals provided by VMware Inc.

Managing storage systems

This section describes how to register, view, refresh, edit, and remove storage systems.

Accessing the Manage Storage Systems screen

Access the Manage Storage Systems screen to register, view, refresh, edit, and remove storage systems.

Procedure

1. Enter the VASA Provider URL in your browser:

   `https://VASA-Provider-IP-Address:50001/`

2. Enter the vCenter SSO account and password in the Web UI window according to , and then click **Login**.
3. Click **Manage Storage Systems**.

Registering storage systems

You must register storage systems in the VASA Provider to pass information to VMware vSphere.

Procedure

1. Click **Manage Storage Systems**.
2. Click **Add Storage Systems**.
3. Enter storage system information.

Select the model of the storage system to be registered and then perform the appropriate procedure as follows:

- For VSP, HUS VM, VSP G1000, G1500, VSP F1500, or VSP 5000 series:

  Enter information about the storage system and then click **OK**.

- For VSP G200, G400, G600, G800, VSP F400, F600, F800, or VSP E series:

  a. Enter information about the storage system and then click **Discover**.
  b. Select the storage system to be registered and then click **OK**.

- For VSP G350, G370, G700, G900, or VSP F350, F370, F700, F900:

  a. Select **SVP** or **Configuration manager REST API**.

     If you want to use vVols, select **SVP**.

  b. Enter information about the storage system and then click **Discover**.
  c. Select the storage system to be registered and then click **OK**.

To register storage systems, use a user account in the **Administrator User Group**.

> **Note:** You must create a user for exclusive use by the VASA Provider. When non-VASA Provider users log in to a storage system during vVol operations, vVol performance may be affected.

Refreshing storage system information

If the configuration of a storage system has changed, you must refresh the storage system information registered in the VASA Provider.

Procedure

1. Click **Manage Storage Systems**.
2. Select the check box corresponding to the storage system whose information want to update.
3. Click **Refresh Storage Systems**.
4. Click **OK**.
5. Click **Reload** and then verify that **Status** is **Completed**.

Editing storage systems

Procedure

1. Click **Manage Storage Systems**.
2. Select the storage system and then click **Edit Storage Systems**.
3. Change the target item and then click **OK**.

Removing storage systems

Before you begin

Delete all of the vVols and storage containers on the storage system before removing the storage system. For information on how to delete vVols and storage containers, see Deleting a storage container (on page 49).

Procedure

1. Open the **Manage Storage Systems** screen.
2. Select the check box of the storage system to be deleted.
3. Click **Remove Storage Systems**.
4. Click **OK**.

Managing storage containers (for vVols)

A storage container is a logical pool, defined by the storage administrator, that stores vVols. The storage container is used when creating a vVols datastore in vCenter Server.

Creating a storage container

Before you begin

Prepare resource groups for storing the vVols in a storage system. For information about the resource group requirements for using vVols, see Configuring storage system resources and resource groups (on page 34).

Procedure

1. Click **Manage Storage Containers**.
2. Click **Create Storage Container**.
3. In **Step1**, specify the following items.

   - **Name**: Enter any storage container name.

   - **Storage Systems**: Select a model that corresponds to the serial number of the target storage system.

   - **Resource Group**: Select the resource group to be used for the storage container.

4. In **Step2**, select **Not used in Replication**.
5. In **Step3**, set Capability Profile.

   a. Select the check box of the pool for which Capability Profile is to be set, and then click **Define Profile**.

   b. In **Name**, enter any profile name.

   c. In the **Managed Capabilities** tab, select the check box of the capability to be set.

   d. Click **OK**.

Chapter 5: Using the VASA Provider

> ⚠️ **Caution:**
>
> If you set a different VM Storage Policy between pools, a good practice is to set one Storage Container per policy. If you set different profiles to multiple pools in one Storage Container, the VM cannot be transferred among the pools. See <u>Restrictions and considerations for vVols Environments (on page 18)</u>.

> 📄 **Note:** Compression and Deduplication, which are User Defined Capabilities, are only accessible when using Tag-based Storage Capability. However, these capabilities are not supported when vVols are used.
>
> For example, the compression function is enabled when the **Compression** value is **Yes**. The FMD compression function is enabled when the **Compression** value is **Accelerated**.

6. Click **Submit**.

> 📄 **Note:** Tag-based storage policy profiles will be automatically set for any VMFS datastores backed by LDEVs residing in the available pool. User Defined Capabilities apply only to profiles associated with a Tag-based Storage Capability.

Displaying storage container information

You can view storage container profiles and related vVols information.

> 📄 **Note:**
>
> - If FMD compression is enabled, Pool Capacity and Physical Pool Capacity might appear in the pool information in Storage Navigator. In such cases, VASA Provider calculates the capacity of the storage container based on the value of Physical Pool Capacity.
>
> - If the total size of the volumes created in a pool exceeds the value of Physical Pool Capacity, the value of Free of Logical Pool Capacity for the storage container might become a negative value. In such cases, increase the value of Subscription Limit in the pool settings of Storage Navigator.

Procedure

1. Click **Manage Storage Containers**.
2. Select a storage container.
3. Click a tab to view specific information about the storage container.

   - **Capability Profile** tab: view Capability Profile information

   - **Default Profile** tab: view default profile information

   - **vVols** tab: view SLUs and bound ALUs managed by the storage container

Editing a storage container

Chapter 5: Using the VASA Provider

Procedure

1. Click **Manage Storage Containers**.
2. Click **Edit Storage Container**.
3. Modify the storage container information. For more information, see <u>Creating a storage container (on page 47)</u>.
4. Click **Submit**.

Deleting a storage container

Before you begin

Verify that all vVols residing in the storage container have been deleted. Before deleting a storage container, first delete or migrate the VMs residing on its vVols datastore, then delete the vVols datastore itself.

Procedure

1. Click **Manage Storage Containers**.
2. Click **Delete Storage Container**.
3. Click **Submit**.

> 📄 **Note:** Resource groups will remain even after deleting a storage container. For information about how to delete resource groups, see the manual for the storage system being used.

Managing LDEVs for VMFS

You can manage tag-based policy LDEVs (datastores) that are visible to VMware ESXi. You can also set Tag-based Storage Policy values for LDEVs.

Note that an LDEV will inherit the Capabilities of its underlying pool if that pool has been assigned a storage Capability Profile. You can further customize tags at an LDEV level by performing the following procedure.

Accessing the Manage Volumes screen

Procedure

1. Click **Manage Storage Systems**.
2. Click **LDEV's** for a storage system.

Creating an LDEV storage profile

Before you begin

Before you define an LDEV storage profile, a VMFS datastore made up of LDEVs must exist.

Procedure

1. Refer to <u>Accessing the Manage Volumes screen (on page 49)</u>, and open the **Manage Volumes** screen.

2. Select an LDEV, then click **Define Profile**.

3. Click **Submit** after setting the Capability Profile (Profile Tag). To see a list of available Capability Profile values, click **Capability Schema**.

> 📄 **Note:**
>
> - Storage profiles reside in the same vCenter Server instance used by the VASA Provider for SSO authentication.
>
> - It may take up to five minutes for the Tag-based Storage Policy to be reflected in vCenter Server.
>
> - To set the storage profile for each pool, create a storage container and then set a storage profile for the pool. The profile will be applied to all LDEVs used for VMFS datastores which reside in the pool.

Editing an LDEV storage profile

Procedure

1. Refer to <u>Accessing the Manage Volumes screen (on page 49)</u>, and open the **Manage Volumes** screen.

2. Select an LDEV, then click **Define Profile**.

3. Modify the Capability Profile (Profile Tag) value, and click **Submit**.

> 📄 **Note:** It may take up to five minutes for updated Tag-based Storage Policy information to appear in vCenter Server.

Deleting an LDEV storage profile

Procedure

1. Refer to <u>Accessing the Manage Volumes screen (on page 49)</u>, and open the **Manage Volumes** screen.

2. Select an LDEV, then click **Define Profile**.

3. Deselect all set values, and click **Submit**.

> 📄 **Note:** It may take up to five minutes for updated Tag-based Storage Policy information to appear in vCenter Server.

Displaying Storage System Pool Information

This displays a list of pools on the storage system for reference when using vVols.

Procedure

1. Click **Manage Storage Systems**.

2. Click **Pool's** for the Storage system.

Managing the Capability Schema

The Capability Schema is a list of settings you can set to create a Capability Profile.

Displaying the Capability Schema

You can view the Capability Schema.

Procedure

1. Enter the VASA Provider URL in your browser:

   `https://VASA-Provider-IP-Address:50001/`

2. In the Web UI window, enter the vCenter SSO account and password according to Logging in to the Web UI (on page 30), and then click **Login**.

3. Click **Capability Schema**.

   Note: Compression and Deduplication, which are User Defined Capabilities, are only accessible when using Tag-based Storage Capability. However, these capabilities are not supported when vVols are used.

   For example, the compression function is enabled when the **Compression** value is **Yes**. The FMD compression function is enabled when the **Compression** value is **Accelerated**.

Creating User Defined Capabilities

Procedure

1. Open the **Capability Schema** screen.

2. Select **Manage Capabilities**.

3. Select **Create Capability**.

4. In **Step1**, enter a name and description for the Capability.

5. In **Step2**, enter a Capability value.

   a. To create new value, select **Add Value**.

   b. To change an existing value, click the value, then select **Edit Value**.

   c. To delete an existing value, click the value, then select **Delete Values**.

6. Click **Submit**.

Editing User Defined Capabilities

Procedure

1. Open the **Capability Schema** screen.
2. Select **Manage Capabilities**.
3. Select the Capability, then click **Edit Capability**.
4. To edit the name or description of the Capability, go to **Step1**.
5. To enter a Capability value, go to **Step2**.
   a. To create new value, select **Add Value**.
   b. To change an existing value, click the value, then select **Edit Value**.
   c. To delete an existing value, click the value, then select **Delete Values**.
6. Click **Submit**.

Deleting User Defined Capabilities

Procedure

1. Open the **Capability Schema** screen.
2. Select **Manage Capabilities**.
3. Select the Capability, then click **Delete Capability**.
4. Click **Submit**.

> ⚠️ **Caution:** Verify that there are no Storage Profile configurations that use the User Defined Capabilities to be deleted. It may be necessary to re-configure a number of Storage Profile settings prior to deleting the User Defined Capabilities.

Enabling vVols Policy Compliance

If you enable vVols Policy Compliance, vVols (SLUs) are automatically stored in the appropriate tiers based on the user-specified Storage Capabilities. To check the correspondence between Storage Capabilities and the tiers in which datastores are stored, check the VM Policy in the table for the Enable vVol Policy Compliance check box on the Capability Schema screen.

For information about operating procedures when this function is enabled, see .

Before you begin

- The storage system is in the VSP E series, the VSP F series, the VSP G series, or the VSP 5000 series.
- Dynamic Tiering is enabled.
- If you want to use active flash, it is enabled.

Procedure

1. Open the **Capability Schema** screen.

2. Select the **Enable vVol Policy Compliance** check box.

3. Click **Apply Policy Compliance**.

Enabling VMFS Policy Compliance

If you enable VMFS Policy Compliance, VMFS datastores are automatically stored in the appropriate tiers based on the user-specified Storage Capabilities. To check the correspondence between Storage Capabilities and the tiers in which datastores are stored, check VM Policy in the table for the Enable VMFS Policy Compliance check box on the Capability Schema screen.

For information about operating procedures when this function is enabled, see <u>Using VMFS Policy Compliance (on page 43)</u>.

Before you begin

- The storage system is in the VSP E series, the VSP F series, the VSP G series, or the VSP 5000 series.

- The configuration uses an SVP.

- Dynamic Tiering is enabled.

- If you want to use active flash, it is enabled.

- The storage system's tiering policy IDs 29, 30, and 31 are not being used.

  When you enable VMFS Policy Compliance, tiering policies are created with the tiering policy IDs 29, 30, and 31.

Procedure

1. Open the **Capability Schema** screen.

2. Select the **Enable VMFS Policy Compliance** check box.

3. Click **Apply Policy Compliance**.

Managing replication groups (for vVols Replication)

A replication group is a logical grouping to which vVols Replication is applied. Create replication groups based on Protector data flows.

Accessing the Replication Groups screen

Access the Replication Groups screen to add, delete, or verify replication groups.

Procedure

1. Enter the VASA Provider URL in your browser:

   `https://VASA-Provider-IP-Address:50001/`

2. Enter the vCenter SSO credentials by performing the procedure in <u>Logging in to the Web UI (on page 30)</u>, and then click **Login**.

3. Click **Replication Groups**.

Chapter 5: Using the VASA Provider

Creating a replication group

Create a replication group to be used for vVols Replication. For details, see the *Hitachi Storage (VASA) Provider for VMware vCenter vVols Replication Guide*.

Updating a replication group

If the configuration of a Protector data flow is changed, you must refresh the Protector information in VASA Provider.

Procedure

1. Click **Replication Groups**.
2. Click **Refresh Protector information**.

Deleting a replication group

To dispose of a vVols Replication environment, delete the replication group. For details, see the *Hitachi Storage (VASA) Provider for VMware vCenter vVols Replication Guide*.

> 💡 **Tip:**
>
> - To delete a replication group after a Forced Failover is performed, refer to the procedure for performing a Forced Failover in *Hitachi Storage (VASA) Provider for VMware vCenter vVols Replication Guide* to delete the replication group.
>
> - Forced Delete Replication Group can be used only after a Forced Failover is performed.

Chapter 6: Additional Configuration Options

The VASA Provider provides the following additional configuration options. Specify these options according to the environment where you plan to use the VASA Provider.

Setting up High Availability

The VASA Provider supports high availability through the VMware vSphere High Availability (vSphere HA) or VMware vSphere Fault Tolerance (vSphere FT) functions. Since the vVols/ VASA environment may become unavailable if an error occurs with the VASA Provider, we recommend that you create a high availability setup.

> **Note:**
>
> - To prepare for database errors caused by unexpected errors in the VASA Provider, set up periodic backups. See Backing up and restoring a database (on page 55).
>
> - The use of vSphere FT may cause a reduction in performance. Subsequently, if an error occurs, adjust the environment using the following procedure provided by VMware.
>
>   - Lower the number of run operations in the vVols environment.
>
>   - Migrate the VASA Provider VM to an ESXi host with better performance.
>
> For details about various functions, see the manuals provided by VMware, Inc.

Backing up and restoring a database

VASA Provider stores, in its database, information related to vVols metadata. For VASA Provider, we recommend using VMDK on a VMFS, NFS, or vSAN datastore created on a storage system.

VASA Provider stores database logs and a full backup on this external VMDK. A full backup is performed once a day. The logs and full backup are retained for up to 30 days. This allows VASA Provider to restore data to any point in time up to two minutes before a failure if the primary VASA database is unavailable. (The database switches logs every two minutes.)

By default, the backup data is stored in `/opt/VVolDataBackup`.
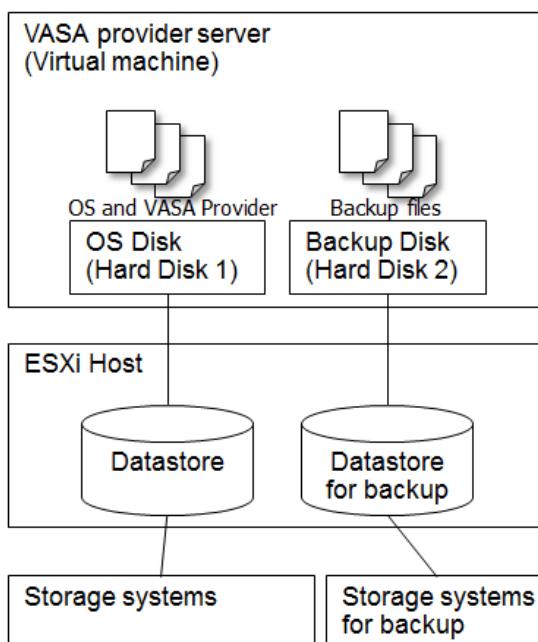
> 📄 **Note:** You can use this function to restore a database to its state at the time when a backup was created. You cannot restore changes to the VASA Provider status that were made after the backup was created.
>
> To ensure that all changes to the VASA Provider status can be restored, after performing an operation that changes the status, manually create a backup.

By default, these backup files are also stored in the VASA Provider VM's guest operating system, on a filesystem located on a second virtual disk. We recommend to keep the database VMDK and the backup VMDK on different storage systems to mitigate the risk of a single point of failure. You can set up this configuration during installation.

If both the database and its backups are lost, it will not be possible to recover the associated vVols environment. To mitigate this risk, configure a separate storage system for backup.

By configuring the VASA Provider VM with a virtual disk backed by a separate storage system, and configuring its backups to reside there, this single point of failure is eliminated.

Follow the procedure listed below to configure database resiliency.

Procedure

1. Prepare a datastore on a storage system that is separate from the storage system used to back the VASA Provider VM itself.
2. Relocate the virtual disk at the backup destination to the new datastore.

   For the OVA VASA Provider version: After deployment, relocate the VASA Provider VM's second virtual disk (used for backups) to a datastore residing on a separate storage system.

> ⚠️ **Caution:** In an environment containing a large number of vVols, backups might fail if the backup disk does not have sufficient available capacity. Verify the available capacity and, if necessary, increase the capacity of the backup disk.For details about how to increase the capacity of the backup disk, see Expanding the capacity of the backup disk (on page 60).

Relocating the backup disk to a datastore on a separate storage system

Before you begin

- Prepare a datastore on a separate storage system for backup disk storage.

- Deploy the VASA Provider.

- Power off the VASA Provider virtual machine.

Procedure

1. Log in to vSphere Client, and then go to **VMs and Templates**.
2. Right-click on the VASA Provider VM, select **Migrate**.
3. In the Migrate wizard, select **Change storage only**, click **NEXT**.
4. Select the storage system to which the virtual machine is to be migrated, and then click **NEXT**.
5. Verify the settings, click **FINISH**.
6. After relocating the virtual disk, restart the VASA Provider VM.

Creating a backup manually

VASA Provider automatically backs up the database. You can also manually create a backup.

Run the following command to manually create a backup:

```
# su postgres
$ /vpdata/pg_cron.sh
```

Restoring the backup file

Before you begin

- Verify that you have a backup for the VASA Provider database.

- Prepare a VASA Provider that is the same version as the VASA Provider used when the problem occurred. The items listed below must be the same as the settings of the VASA Provider for which the problem occurred.

    - Time zone

      If vVols Replication is enabled, configure the NTP server settings for the local site and the remote site, and make sure that the times at the two sites are synchronized.

    - IP address and host name

    - Time

- Power off the VASA Provider virtual machine.

Procedure

1. Log in to vSphere Client, and then go to **VMs and Templates**.
2. Right-click on the VASA Provider VM, select **Edit Settings**.
3. Hover your mouse pointer over **Hard Disk 2**. Select the **X** that appears to delete the disk.
4. Click **OK**, close the **Edit Settings** window.
5. When vSphere has finished reconfiguring the VASA Provider VM, right-click on it again, and select **Edit Settings**.
6. Select **Existing Hard Disk** from the **New device** list, click **Add**.
7. In the **Select File** window, select the backup disk (VMDK file) for the VASA Provider that had the problem, click **OK**.
8. Click **OK** to close the **Edit Settings** window.
9. Restart the VASA Provider VM.
10. Log in to the guest operating system of the VASA Provider VM as the root user (root/ password).
11. Stop the VASA Provider service with the following command:

    ```
    # /usr/local/hitachivp-b/tomcat_vp_b stop
    ```

12. Change to the postgres user.

    ```
    # su postgres
    ```

13. Stop the PostgreSQL service.
    a. Run the following command, and identify the output `service` file.

    ```
    # systemctl list-unit-files -t service | grep postgres
    postgresql-<version>.service                    enabled
    ```

    b. Run the following command. Specify the `service` file that was output when you ran the preceding command.

```
$ systemctl stop postgresql-<version>.service
```

14. Check the information about the backup.

```
$ pg_rman show
```

15. Restore the database from the backup.

The database is restored to the time when the system was specified. The time zones must be the same.

```
$ pg_rman restore
```

If you do not specify a date and time, the database will be restored by using the latest backup.

If you want to specify a date and time, specify the following option. Specify the date and time and the timeline (TLI) that you checked in step 14.

```
--recovery-target-time 'YYYY-MM-DD HH:MM:SS' --recovery-target-timeline TLI
```

Example:

```
--recovery-target-time '2020-11-10 08:04:38' --recovery-target-timeline 1
```

16. Open the `/vpdata/postgresql.conf` file in a text editor, and then change `recovery_target_action` to the following.

```
recovery_target_action = 'promote'
```

17. Open the `/vpdata/pg_rman_recovery.conf` file in a text editor, and then change `restore_command` to the following.

```
restore_command = 'gunzip < /opt/VVolDataBackup/wal/%f.gz > /vpdata/pg_wal/%f'
```

18. Start the PostgreSQL service.

```
$ systemctl start postgresql-<version>.service
```

19. Change to the root user.

```
$ exit
```

20. Start the VASA Provider service.

```
 # /usr/local/hitachivp-b/tomcat_vp_b start
```

21. On the vSphere Client, cancel the existing VASA Provider registration information.

    a. Log in to vSphere Client, and then navigate to vCenter Server.

    b. In the right pane, select the **Configure** tab, and then click **Storage Providers**.

    c. Select the registered VASA Provider, and then click **X Remove**.

    d. In the confirmation window, click **Yes**.

22. Register the new VASA Provider.

Expanding the capacity of the backup disk

In an environment containing a large number of vVols, the available capacity of the backup disk for VASA Provider might not be sufficient. Expand the capacity of the backup disk as needed.

Procedure

1. Log in to vSphere Client, and then go to **VMs and Templates**.
2. Right-click on the VASA Provider VM, and select **Edit Settings**.
3. Change the value of **Hard Disk 2** to the value after the capacity is expanded.
4. Click **OK** to close the **Edit Settings** window.
5. Log in to the guest operating system of the VASA Provider VM as the root user (root/ password).
6. Use the following command to verify that the capacity has expanded.

```
# fdisk -l
```

7. Use the following command to expand the capacity of the physical volume.

```
# pvresize /dev/sdb
```

8. Use the following command to verify that the capacity of the physical volume (PSize) has expanded.

```
# pvs
```

9. Use the following command to verify that the available capacity of the volume group (VFree) has expanded.

```
# vgs -o name,vgfree
```

10. Use the following command to expand the capacity of the logical volume.

```
# lvextend -r -l +100%FREE <logical_volume_name>
```

Specification example:

```
# lvextend -r -l +100%FREE /dev/vg_backup/lv_backup
```

11. Use the following command to verify that the capacity of the logical volume has expanded.

   ```
   # lvscan
   ```

12. Use the following command to verify that the capacity of the backup space (Size/Avail) has expanded.

   ```
   # df -Th
   ```

VASA Provider migration

If you migrate or reconfigure a VASA Provider, you must migrate the data containing vVols information. Follow the procedure described below to migrate the data.

> ⚠️ **Caution:**
>
> - The versions of the migration-source and migration-destination VASA Providers must be the same.
>
> - Do not operate the VM during VASA Provider data migration. Though the VM will remain online throughout the migration, it may not function normally until the migration's complete.

Procedure

1. Unregister the pre-migration VASA Provider from VMware vSphere. See <u>Removing the VASA Provider from vCenter Server (on page 38)</u>.
2. Log in as root (root/password) to the guest OS of the pre-migration VASA Provider VM.
3. Stop the VASA Provider.
   ```
   # /usr/local/hitachivp-b/tomcat_vp_b stop
   ```
4. Export the data with the following command:
   ```
   # pg_dumpall -c -p 50003 -U postgres -f pg_dumpall_vpdata.sql
   ```
5. Deploy the post-migration VASA Provider as a separate VM.
6. Copy the exported data `(pg_dumpall_vpdata.sql)` to the guest OS of the post-migration VASA Provider VM.
7. Stop the migration-source VASA Provider.
8. Log in as root (root/password) to the guest OS of the post-migration VASA Provider VM.
9. Stop the VASA Provider.
   ```
   # /usr/local/hitachivp-b/tomcat_vp_b stop
   ```
10. Import the data with the following command:
   ```
   # psql -f pg_dumpall_vpdata.sql -U postgres -p 50003
   ```
11. Start the VASA Provider.
   ```
   # /usr/local/hitachivp-b/tomcat_vp_b start
   ```

12. In an environment where vVols Replication is used, reregister the Remote VASA Provider information.

    For details, see *Configuring a remote connection by using VASA Provider at the local site* and *Configuring a remote connection by using VASA Provider at the remote site*, in the *Hitachi Storage (VASA) Provider for VMware vCenter vVols Replication Guide*.

13. Register the new VASA Provider. See <u>Registering the VASA Provider in vCenter Server (on page 37)</u>.

14. Log in to vSphere Client, and then navigate to vCenter Server.

15. In the right pane, select the **Configure** tab, and then click **Storage Providers**.

16. Select the target VASA Provider, and then click **Rescan**.

Changing VASA Provider credentials

You can change the user name and password of the administrator account used for the VASA Provider.

Procedure

1. Enter the VASA Provider URL in your browser:

   `https://VASA-Provider-IP-Address:50001/`

2. In the Web UI window, enter the vCenter SSO account and password according to <u>Logging in to the Web UI (on page 30)</u>, and then click **Login**.

3. In the Web UI main window, click **Change Credentials**.

4. Provide the following information:

   - Current administrator account's user name and password (currently logged in)

   - New administrator account's user name and password

   - New password confirmation

   The maximum number of characters for credentials is 255. The supported characters are:

   `A-Z a-z 0-9 ! # $ { } * - . = @ ^ | ~ / ? ` `

5. Click **Change Credentials**.

Setting up vCenter SSO Server

VASA Provider uses vCenter SSO for user authentication. To change the vCenter SSO server specified at deployment, follow the procedure below.

Procedure

1. Enter the VASA Provider URL in your browser:

   `https://VASA-Provider-IP-Address:50001/`

2. In the Web UI window, enter the vCenter SSO account and password (or `system` and `manager`) according to <u>Logging in to the Web UI (on page 30)</u>, and then click **Login**.

3. Select **General Settings** from the **Maintenance** menu.

   If you logged in by entering `system` and `manager`, select **Single Sign-on Setting** from the **Maintenance** menu.

4. For **Set vCenter SSO server information**, enter the network IP address or the FQDN.

5. Enter the port number.

6. For **Single Sign-On domain name**, enter the vSphere domain name.

   Use the same domain name of vCenter Server or PSC (Platform Services Controller).

   Default domain name: `vsphere.local`

7. Click **Set**.

> **Important:** If **Set** is disabled, clear the browser's cache, restart the browser, then reconfigure the settings.

Renewing an SSL certificate

SSL certificates have an expiration date. When this expiration date is reached, it is necessary to create a new certificate. There are two ways to create the certificate: by using the Web UI, or by using a script stored in the VASA Provider.

> **Caution:** Unregister the VASA Provider from vCenter Server, when you create SSL certificates. While the VASA Provider is not registered from vCenter Server, VMs that are running will not be affected. However, you cannot perform start, stop, and copy operations while the VASA Provider is not registered.

Renewing an SSL certificate using the Web UI

Procedure

1. Follow the procedure in Removing the VASA Provider from vCenter Server (on page 38).

2. Enter the VASA Provider URL in your browser:

   `https://VASA-Provider-IP-Address:50001/`

3. In the Web UI window, enter the vCenter SSO account and password (or `system` and `manager`) according to Logging in to the Web UI (on page 30), and then click **Login**.

4. Click **Update Certificate** on the Web UI's main page.

5. Select IP address or enter FQDN, then click **Update**.

6. Click **OK** when prompted for verification. The VASA Provider service will restart.

7. Follow the procedure in Registering the VASA Provider in vCenter Server (on page 37).

Renewing an SSL certificate using the script

Procedure

1. Follow the procedure in Removing the VASA Provider from vCenter Server (on page 38).

2. Log in to the guest operating system of the VASA Provider VM as the root user (root/
   password).

3. At the root prompt, enter the following commands:

   ```
   cd /usr/local/hitachivp-b

   ./createCertifications.sh
   ```

4. Restart the VASA Provider service; see

5. Follow the procedure in .

Restarting the VASA Provider service

It may be necessary to restart the VASA Provider service in some cases, such as after a certificate is renewed.

This section explains how to use commands to restart the service. However, you can also restart the service from the Restart Service from the Maintenance menu of the VASA Provider Web UI.

Procedure

1. Run the following commands.

   ```
   # /usr/local/hitachivp-b/tomcat_vp_b stop
   # /usr/local/hitachivp-b/tomcat_vp_b start
   ```

Configuring log output settings

To prevent logs from consuming excessive disk space, the VASA Provider automatically rotates them when they reach a configurable maximum size. It's possible to change both the maximum log file size, and the number of old log files to retain.

Log files subject to rotation include the VASA Provider's (`StorageProvider.log`) and the VASA Provider Web UI's (`VasaWebUi.log`).

Before you begin

- The VASA Provider is installed.
- The VASA Provider VM is powered on.
- Network settings are configured.
- SSL certificates is created.

Procedure

1. Log in to the guest operating system of the VASA Provider VM as a root user (root/
   password).

2. Edit the `hilogger.config` file as desired to change the following parameters.

Item	Description
`MaxBackupIndex`	Indicates the maximum number of log files to retain. Range: 1-255. Default value: 50. Any value outside of the range is treated as the default value.
`MaxFileSize`	Indicates the maximum log file size. Range: 1-100. Default value: 100 MB. Any value outside of the range is treated as the default.

The `hilogger.config` file is located in the following:

For the VASA Provider
```
/usr/local/hitachivp-b/tomcat/webapps/VasaProvider/WEB-INF/
conf
```

For the VASA Provider Web UI
```
/usr/local/hitachivp-b/tomcat/webapps/VasaProviderWebUi/WEB-
INF/conf
```

For the VASA Provider Common Landing Page
```
/usr/local/hitachivp-b/tomcat/webapps/CommonLandingPage/WEB-
INF/conf
```

For details about how to obtain log files, see <u>Downloading the VASA Provider log (on page 70)</u>.

3. Restart the VASA Provider service; see <u>Restarting the VASA Provider service (on page 64)</u>.

Using multiple networks with the VASA Provider

This procedure is required in situations where vCenter Server and one or more storage system SVPs reside in separate networks. If the VASA Provider's unable to access a storage system SVP using the same network interface used to access vCenter Server, add a second network interface to the VASA Provider for SVP access.

Procedure

1. Install the VASA Provider.
2. Choose network settings which will allow the VASA Provider to access vCenter Server.
3. In the VASA Provider VM, add a second vNIC associated with a vSwitch that's uplinked to a network with access to storage system SVPs.

   For more information, see documentation provided by VMware, Inc.
4. Log in to the VASA Provider VM's guest operating system as root (root/password).

5. Within the VASA Provider VM's guest operating system, configure TCP/IP on the VM's second vNIC with settings which will allow access to storage system SVPs. For more information, see documentation provided by Oracle Corporation.

6. Restart the VASA Provider VM.

7. Register the storage system. See <u>Registering storage systems (on page 45)</u>.

> ⚠ **Caution:** After changing the network settings used by the VASA Provider to connect vCenter Server, it may be necessary to create a new SSL certificate.
>
>   a. Log in to the guest operating system of the VASA Provider VM as the root user (root/password).
>
>   b. Open `/usr/local/hitachivp-b/openssl.cnf` with a text editor, and edit the file to include the IP address or the FQDN of the VASA provider.
>
>   Example of adding the IP address:
>
> ```
> IP.1 = 192.168.86.133
> ```
>
>   Example of adding the FQDN:
>
> ```
> DNS.1 = vasaprovider.local.local1
> ```
>
>   c. Run the script as shown, to create a new SSL certificate:
>
> ```
> # /usr/local/hitachivp-b/createCertifications.sh
> ```

Setting quotas for storage containers

You can change the percentage of the capacity of a storage container for which a notification is sent to vCenter Server as follows. The default value is 70%.

> 📄 **Note:** In each of the following cases, the quota value will be 100%.
>
> - The usage rate of the storage container exceeds the current quota value.
> - The quota value is changed to a value less than the usage rate of the storage container.
> - A storage container whose usage rate exceeds the quota value is created.

Procedure

1. Log in to the guest operating system of the VASA Provider VM as the root user (root/password).

2. Open the `VasaProvider.properties` file with a text editor. For `storageContainerQuota`, set a value between 10 and 100. The `VasaProvider.properties` file is located in the following directory:

   `/usr/local/hitachivp-b/tomcat/webapps/VasaProvider/META-INF`

3. Restart the VASA Provider service; see <u>Restarting the VASA Provider service (on page 64)</u>.

Setting alarm levels for VMFS

VASA Provider will enable, in vCenter Server, settings for the warning and alert threshold levels for datastore usage including thin provisioning alarms. These default threshold values can be updated inside VASA Provider. Follow the procedure below.

> 📄 **Note:** If the Full Allocation setting is enabled for LDEVs to be used for VMFS datastores, an alarm will be output because Used(%) for DP volumes is always 100%. If you want to suppress the alarm, set the yellow and red alarm level to 0.

Procedure

1. Log in to vSphere Client, and then go to **Storage**.
2. In the left pane, select the target datastore.
3. In the right pane, select the **Monitor** tab, and then select **Triggered Alarms**.
4. If the alarm exists, select the check box of the alarm and then click **RESET TO GREEN**.
5. Log in to the guest operating system of the VASA Provider VM as the root user (root/password).
6. Back up the properties file.

   ```
   cd /usr/local/hitachivp-b/tomcat/webapps/VasaProvider/META-INF/

   cp VasaProvider.properties VasaProvider.properties.bak
   ```

7. Open the `VasaProvider.properties` file with a text editor.
8. Check the alarm levels that are set in the properties file.

   The alarm levels are set in the following locations.

   ```
   # Determines the alarm level for a yellow alarm.
   # This value must be a value between 0 and 100.
   # Default value is 65.
   service.alarms.level.yellow=90

   # Determines the alarm level for a red alarm.
   # This value must be a value between 0 and 100.
   # Default value is 80.
   service.alarms.level.red=95
   ```

9. Change the alarm levels for yellow and red alarms.

   It is recommended that you set an alarm level no higher than 90 for yellow alarms (default: 65).

   It is recommended that you set an alarm level no higher than 95 for red alarms (default: 80).

10. Restart the VASA Provider service; see <u>Restarting the VASA Provider service (on page 64)</u>

11. It is highly recommended that you run the UNMAP service to free up disk space.

Chapter 7: VASA Provider Troubleshooting

If a problem occurs while you are using VASA Provider, see the Troubleshooting Guide from the VASA Provider Web UI and resolve the problem. If you cannot resolve the problem, collect the logs and contact customer support.

Recovery procedure for situations such as when the VASA Provider service stops because the backup disk runs out of available capacity

If the backup disk of VASA Provider runs out of available capacity, the VASA Provider service stops, and the following problems occur.

- Attempts to log in to the Web UI fails.
- A virtual machine that uses VASA Provider cannot be operated on vCenter Server.
- A VMFS datastore that uses VASA Provider cannot be managed on vCenter Server.

If the above problems occur, perform the following procedure to restore the environment.

Procedure

1. On the vCenter Server, create a clone of the VASA Provider VM.

   Use the clone created here only when it is necessary to restore the environment.

2. Stop the VASA Provider service by using the following command:

   ```
   # /usr/local/hitachivp-b/tomcat_vp_b stop
   ```

3. Delete the following log files to increase the available capacity on the OS disk. Use the wild card character (*) to delete the log files.

   ```
   /var/log/hitachivp-b/VasaProvider
   StorageProvider.log.*
   StorageModule_trace.log.*
   trace.log.*
   ```

4. Expand the capacity of the backup disk. For details on how to expand the capacity, see Expanding the capacity of the backup disk (on page 60).

5. Start the PostgreSQL service.

   a. Run the following command, and identify the output `service` file.

      ```
      # systemctl list-unit-files -t service | grep postgres
      postgresql-<version>.service                    enabled
      ```

b. Run the following command. Specify the `service` file that was output when you ran the preceding command.

```
$ systemctl start postgresql-<version>.service
```

6. Wait about 10 minutes and then check the status of the PostgreSQL service.

Make sure the status is `Active: active (running)`.

```
# systemctl status postgresql-<version>.service
```

7. Restart the VASA Provider service. For details, see Restarting the VASA Provider service (on page 64).

Collecting logs

Logs from the following components should be collected before contacting customer support.

- The VASA Provider

- Pertinent storage systems

- VMware vCenter Server and ESXi

For log file collection methods, see the respective documentation.

Component	Document	Topic
VASA Provider (block)	-	Downloading the VASA Provider log (on page 70)
vCenter Server/ ESXi host	Please see documentation published by VMware, Inc.	-
Storage system	Please see the storage system manuals.	Collect a normal dump file of the storage system. For information about how to collect a dump file, see the *System Administrator Guide*.

Downloading the VASA Provider log

The VASA Provider allows its logs to be downloaded as ZIP files.

Procedure

1. Enter the VASA Provider URL in your browser:

   `https://VASA-Provider-IP-Address:50001/`

2. In the Web UI window, enter the vCenter SSO account and password (or `system` and `manager`) according to Logging in to the Web UI (on page 30), and then click **Login**.

3. In the main Web UI window, click **Download Logs**.
4. Download the log files according to the instructions in your browser.

Hitachi Vantara