Hitachi Virtual Storage Platform One File

File management software release 1.2.0

NAS File OS release 15.3 or later

Management Software Installation and Configuration Guide

This document provides information for installing and configuring the Hitachi Virtual Storage Platform One File management software.

MK-24VSP1F004-03
October 2024

Contents

Preface

This document describes and provides instructions for installing and configuring the Hitachi Virtual Storage Platform One File management software.

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!

Accessing product documentation

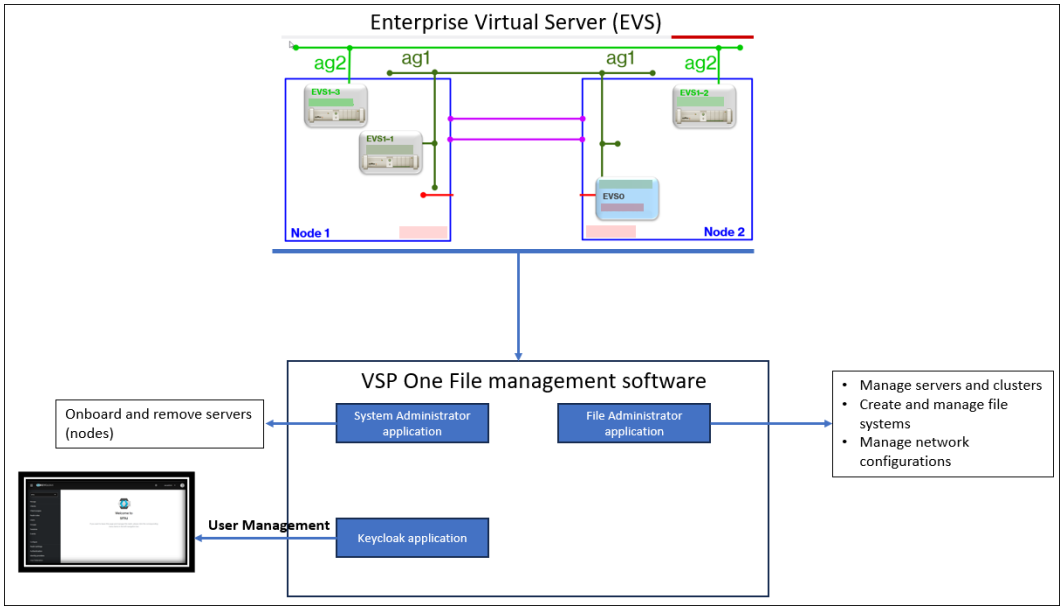
Product user documentation is available on: https://docs.hitachivantara.com. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Chapter 1: Overview

The VSP One File management software helps users to manage Hitachi Virtual Storage Platform One File servers.

System configuration

Hitachi Virtual Storage Platform One File environment consists of one or more physical nodes that can host multiple Enterprise Virtual Servers (EVS).

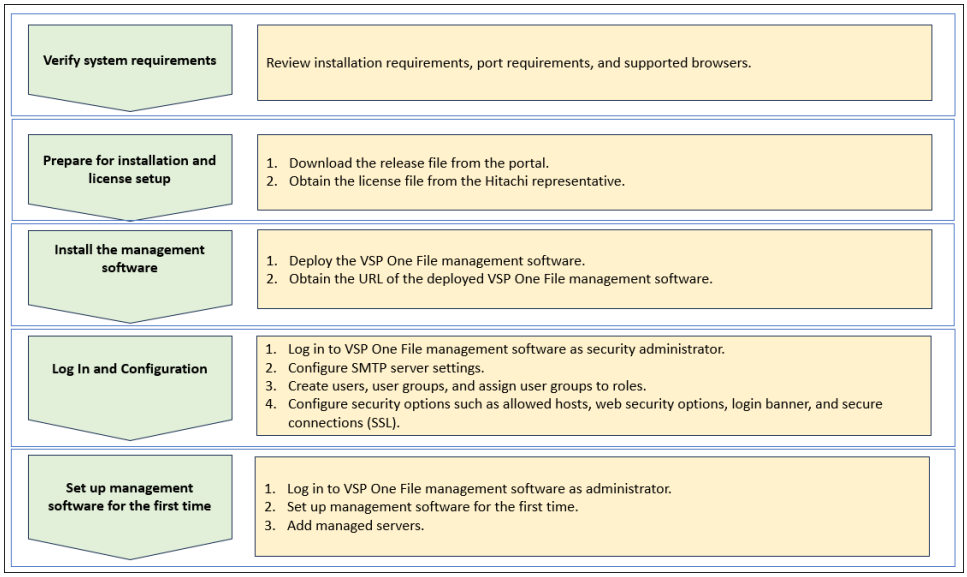


The VSP One File management software consists of the following applications:

- System Administrator: Use this application to onboard and remove servers (nodes), perform tasks like configure name services, backups and restore.
- File Administrator: Use this application to manage servers and clusters, create and manage file systems and enable the configuration of file service protocols.
- Keycloak: Use this application to manage users and their access to applications. Keycloak is a third-party software that provides identity and authorization management.

Workflow for deploying and setting up the VSP One File management software

The following figure shows the workflow for installing and configuring the VSP One File management software:



Chapter 2: System requirements

This module provides the system requirements for installation.

Installation requirements

The following table lists the minimum resource requirements for installation.

Category	Requirements
CPU	Intel x86_64 or AMD 64-bit CPU with at least 4 CPU cores (1 CPU core per managed server or cluster recommended).
Memory	Minimum of 12 GiB or 1 GiB per managed server or cluster, if higher.
Storage	100 GiB of hard drive space.
Network	1 GigE network adapter.
IP address	IP addresses used to connect to the VSP One File management software.  **Note:** Each virtual machine you deploy requires at least one IP address for management UI access.
Virtual machine host	VMware vSphere® ESXi version 7.0u2 or later. Microsoft® Hyper-V Manager version 10.0.22621.1 or later. Kernel-based Virtual Machine (KVM) Virtual Machine Manager 1:3.2.0-3 or later.
Memory for virtual machine host	32 GB

 **Note:** The physical hardware should exceed the minimum requirements so that the host has resources beyond those allocated to the virtual machine. In particular, the host should have more physical RAM than is allocated to the virtual management software.

The latency of the VSP One File management software acting as a quorum device for a VSP One File cluster must be less than five seconds. If the measured latency is near five seconds, you should reconsider deploying the VSP One File management software.

Support for the VSP One File management software running on Debian

The VSP One File management software runs on a Hitachi Vantara customized version of Debian Linux version 11 and supported on VMware vSphere ESXi, Microsoft Hyper-V, and KVM.

Port requirements

The tables below describe the listening and destination default ports in use for services on the VSP One File server and management software.

VSP One File server listening ports

Port/Protocol	Service
21/TCP	FTP
22/TCP	SSH
25/TCP	SMTP relay
80/TCP	HTTP
111/TCP/UDP	Port mapper
135TCP	DCERPC endpoint info
161/UDP	SNMP agent
202/TCP	VSS
206/TCP	SSC
443/TCP	HTTP over TLS
445/TCP	SMB over TCP
762/TCP/UDP	rquota
800/TCP/UDP	RPC
2049/TCP/UDP	NFS
3205/TCP	iSNS
3260/TCP	iSCSI
4045/TCP/UDP	lockd
4048/TCP/UDP	mountd
4050/TCP/UDP	statd
8444/TCP	REST API

Port/Protocol	Service
10000/TCP	NDMP
11106/TCP	Statistics server
34741/TCP/UDP	VAAI
59515/UDP	Quorum service
59516/UDP	Quorum service
59535/UDP	Cluster communication
59536/UDP	Cluster communication
59550/TCP	Object replication

VSP One File server destination ports

Port/Protocol	Service
25/TCP	SMTP relay
53/TCP/UDP	DNS
80/TCP	Data Migrator to Cloud
443/TCP	Data Migrator to Cloud
88/TCP/UDP	Kerberos
123/UDP	NTP
162/UDP	SNMP traps
389/TCP/UDP	LDAP
445/TCP	SMB over TCP
464/TCP/UDP	Kerberos Password Change
636/TCP/UDP	LDAP over TLS
1344/TCP	ICAP AV
2049/TCP/UDP	NFS
4048/TCP/UDP	mountd
59550/TCP	Object replication

VSP One File management software listening ports

Port/Protocol	Service
22/TCP	SSH
80/TCP	VSP One File management software UI (HTTP)
443/TCP	VSP One File management software UI (HTTP over TLS)
59515/UDP	Quorum Service
59516/UDP	Quorum Service

VSP One File management software destination ports

Port/Protocol	Service
25/TCP	SMTP relay
53/TCP	DNS
123/UDP	NTP
201/TCP	SSC
206/TCP	SSC
389/TCP	LDAP (unencrypted connections)
636/TCP	LDAPS
8444/TCP	REST API
10000/TCP	NDMP

Supported browsers

The VSP One File management software applications support these web browsers:

Web browser	Version
Microsoft Edge	Version 119 or later
Mozilla Firefox	Version 119 or later
Google Chrome	Version 118 or later

The VSP One File management software uses cookies and sessions to remember user selections on various pages. Therefore, open only one web browser window or tab per workstation or computer. If multiple tabs or windows are opened from the same workstation, changes made in one tab or window might affect the other tabs or windows.

Chapter 3: Downloading the VSP One File management software

You can access the VSP One File management software downloads, including important updates made after the release of the software, from the Hitachi Vantara Support website.

Procedure

1. Log in to Hitachi Vantara Support.
2. Click **Download Products and Updates**.
3. On the **Downloads** page, click **Hardware Download**.
4. Click **VSP One File 30 Series**, and then select **File Management Software** in the **Components** list.
5. Identify the installation file for the management software as applicable for the hypervisor that you are using for VSP One File, and then click **Download**.
6. Review the **End User License Agreement**, and then click **Continue** to start the download.

Chapter 4: Installing the VSP One File management software on VMware ESXi

You can install the VSP One File management software on a virtual machine by deploying the VSP One File installation file on a VMware vSphere ESXi™ host.

If the vSphere ESXi host is not already installed and operational, install it on the bare metal host machine.

Use a web browser to access the vSphere Client, which manages the vSphere ESXi host and virtual machines.

Deploying the VSP One File management software operating system on VMware vSphere ESXi

Deploy and map the pre-configured VSP One File management software operating system (OS) template.

Before you begin

Download the VSP One File installation file for the latest release to a local system. For instructions about how to download the file, see Downloading the VSP One File management software (on page 13).

Procedure

1. From a Firmware vSphere client, log in to the Firmware ESXi host server.
2. Right-click a Firmware ESXi host and select **Deploy OVF template**.
3. Browse to the location of the VSP One File management software installation file that you downloaded, and then click **Next**.
4. Enter a name of the virtual machine and the target location where you want to create the virtual machine, and then click **Next**.
5. Select the destination computer resource (host), and then click **Next**.
6. Review the details of the virtual machine, and then click **Next**.
7. Select the storage for the configuration and disk files, and then click **Next**.

   Note: Make sure to check that **Thin Provision** is selected as the virtual disk format.
8. Select the destination network for each source network and then click **Next**.

9. Customize the VSP One File management software OS template by setting **User Name**, **User Login Password**, **Root Login Password**, **Hostname**, **IP Address**, **Netmask**, **Gateway**, **DNS**, **NTP server**, and **Time Zone**, and then click **Next**.

   Note: Valid hostnames consist of letters (a-z, A-Z), numbers (0-9), and hyphens (-). Examples of valid host names are smu-vm1, 123-valid-vm1, smu-integration, smuvm.

   The user login password and the root login password must be at least eight characters and must contain at least one uppercase letter, number, and special character. For example, Password@123.

   If no NTP servers are added, the VSP One File management software OS inherits the date, time, and time zone from the virtual machine. By default, the time zone is set to UTC.

10. Click **Finish** to deploy the VSP One File OS template.

Installing the VSP One File management software VMware vSphere ESXi

After you deploy the VSP One File management software OS template, start and log in to the newly created virtual machine to initiate the installation of the management software.

Procedure

1. From the VMware vSphere client, start the VSP One File virtual machine.
2. Start the virtual machine web console.
3. Log on to Debian with the username and password created in Deploying the VSP One File management software operating system on VMware vSphere ESXi (on page 14). After you log on, the VSP One File management software installation starts automatically.
4. To view the installation progress, run the following command:

   ```
   tail -f /var/log/smu-install.log
   ```

5. When the installation is complete, note the IP Address to access the VSP One File management software.

Chapter 5: Installing the VSP One File management software on Hyper-V

You can install the VSP One File management software on a virtual machine by deploying the installation file on Hyper-V.

If Hyper-V is not already installed and operational, install it on the bare metal host machine.

Use a web browser to access Hyper-V Manager, which manages Hyper-V Server and virtual machines.

Deploying the VSP One File management software on Hyper-V

Deploy the VSP One File management software operating system (OS).

Before you begin

Download the VSP One File installation file for the latest release to a local system. For instructions about how to download the file, see Downloading the VSP One File management software (on page 13).

Procedure

1. Start Hyper-V Manager, and click **Action** > **New** > **Virtual Machine**.
2. In the **New Virtual Machine** wizard, review the information in the **Before You Begin** page, and then click **Next**.
3. On the **Specify Name and Location** page, enter a name for the virtual machine, create a folder or use the default folder for storing the virtual machine files, and then click **Next**.
4. On the **Specify Generation** page, click **Generation 1**, and then click **Next**.
5. On the **Assign Memory** page, enter a startup memory greater than 8 MB, and then click **Next**.
6. On the **Configure Networking** page, select a network switch, and then click **Next**.
7. On the **Connect Virtual Hard Disk** page, click **Use an existing virtual hard disk**, enter the path to the VSP One File installation file that you downloaded, and then click **Next**.
8. On the **Completing the New Virtual Machine Wizard** page, review the summary information, and then click **Finish** to create the virtual machine.
9. Right-click the new virtual machine, and then click **Settings**.
10. Expand **Hardware**, and then click **Processor**.
11. Set the number of virtual processors to a minimum of 4, and then click **OK**.

12. Right-click the virtual machine and click **Connect** to open the **Virtual Machine Connection** window.
13. Click **Actions** > **Start** to start the virtual machine.
14. At the `Do you want to configure DHCP` prompt, specify whether you want to use the Dynamic Host Configuration Protocol (DHCP) to automatically configure the IP address and other network configuration parameters for the virtual machine.
    - To use DHCP, enter `yes`. At the prompts, enter the following information:
      - Username
      - Password
      - Hostname
    - To configure the IP address and network configuration parameters manually, enter `no`. At the prompts, enter the following information:
      - Username
      - Password
      - Hostname
      - IP address
      - Netmask
      - Gateway IP address
      - DNS server IP address
      - Domain name
      - Timezone setup (`yes` or `no`)

        If you enter `yes`, complete the information at the prompts to set the timezone.

Result

The installation completes. Login information and the IP addresses for the virtual machine are shown.

Installing the VSP One File management software on Hyper-V

After you deploy the VSP One File management software OS, start and log in to the newly created virtual machine to install the management software.

Procedure

1. In Hyper-V Manager, start the VSP One File virtual machine.
2. Open the **Virtual Machine Connection** window.
3. Log on to Debian with the username and password created in Deploying the VSP One File management software on Hyper-V (on page 16).
   After you log in, the VSP One File management software installation starts automatically.

4. To view the installation progress, run the following command:

```
tail -f /var/log/smu-install.log
```

5. When the installation is complete, note the IP address to access the VSP One File management software.

Chapter 6: Installing the VSP One File management software on KVM

You can install the VSP One File management software on a virtual machine by deploying the VSP One File installation file on a Kernel-based Virtual Machine (KVM) hypervisor.

If KVM is not already installed and operational, install it on the bare metal host machine.

Use a web browser to access Virtual Machine Manager, which manages KVM and virtual machines.

Deploying the VSP One File management software on KVM

Deploy the VSP One File management software operating system (OS).

Before you begin

Download the VSP One File installation file for the latest release to a local system. For instructions about how to download the file, see Downloading the VSP One File management software (on page 13).

Procedure

1. Start Virtual Machine Manager, and click **File** > **New VM**.
2. On the **Create New Virtual Machine** page, click **Import existing disk image**, and then click **Forward**.
3. On the **Locate or create storage volume** page, select the VSP One File installation file, and then click **Choose Volume**.
4. On the **Create New Virtual Machine (Step 2)** page, select **Debian 10**, and then click **Forward**.
5. On the **Create New Virtual Machine (Step 3)** page, set the memory to a minimum of 8 MiB and the CPUs to 4, and then click **Forward**.
6. On the **Create New Virtual Machine (Step 4)** page, select the network, and then click **Finish**.

7. At the `Do you want to configure DHCP` prompt, specify whether you want to use the Dynamic Host Configuration Protocol (DHCP) to automatically configure the IP address and other network configuration parameters for the virtual machine.
   - To use DHCP, enter `yes`. At the prompts, enter the following information:
     - Username
     - Password
     - Hostname
   - To configure the IP address and network configuration parameters manually, enter `no`. At the prompts, enter the following information:
     - Username
     - Password
     - Hostname
     - IP address
     - Netmask
     - Gateway IP address
     - DNS server IP address
     - Domain name
     - Timezone setup (`yes` or `no`)

       If you enter `yes`, complete the information at the prompts to set the timezone.

Result

The installation completes. Login information and the IP addresses for the virtual machine are shown.

Installing the VSP One File management software on KVM

After you deploy the VSP One File management software OS, start and log in to the newly created virtual machine to install the management software.

Procedure

1. In Virtual Machine Manager, start the VSP One File virtual machine.
2. Click **File** > **Add Connection**
3. Log on to Debian with the username and password created in Deploying the VSP One File management software on KVM (on page 19).
   After you log in, the VSP One File management software installation starts automatically.
4. To view the installation progress, run the following command:

```
tail -f /var/log/smu-install.log
```

5. When the installation is complete, note the IP address to access the VSP One File management software.

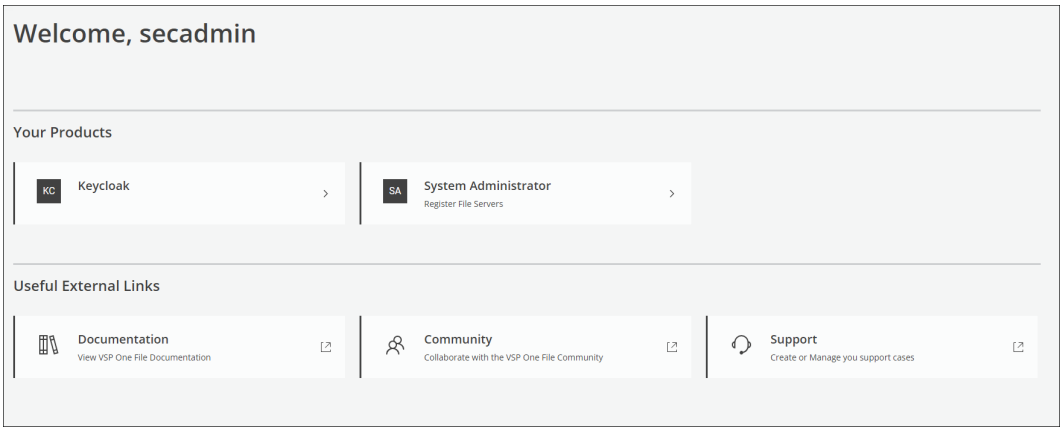
Chapter 7: Log in to the VSP One File management software for the first time as security administrator

To access the VSP One File management software for the first time, obtain default login credentials from your system administrator. You are prompted to change the default password at initial login.

Procedure

1. In your browser, enter the VSP One File URL: `https://server-IP-address`
2. Log in using your default secadmin credentials. User ID: `secadmin` and Password: `nasadmin`
3. Change the password when prompted. The password must contain uppercase and lowercase letters, numbers, and special characters.

   The landing page is displayed.



4. From the landing page:
   - Use **Keycloak** to configure SMTP settings, create users, user groups, and assign user groups to roles. The SMTP settings configuration details are described in Configuring SMTP settings (on page 23) and the user configuration details are described in Configuring users (on page 25).
   - Use **System Administrator** to configure the security options (on page 29) as allowed hosts, web security options, login banner, audit logs, and secure connections (SSL).

Adding email address to security administrator user account

Adding an email address to the security administrator (secadmin) user account enables receiving emails for password resets and verification.

Before you begin

Make sure that you are logged in to the VSP One File management software as security administrator (secadmin) and start Keycloak.

Procedure

1. Navigate to **Manage** > **Users**.
2. In the **Users** page, click the **secadmin** user.
3. In the **secadmin** page, make sure that **Email verified** is set to yes.
4. In the **General** section, enter the email address of the security administrator, and then click **Save**.

Next steps

After adding an email address to the security administrator (secadmin) user account, configure the SMTP settings. For more information, see Configuring SMTP settings (on page 23).

Configuring SMTP settings

Configure the SMTP settings in Keycloak to receive emails from the VSP One File management software. Once the SMTP settings are configured, VSP One File management software will send a password reset link to configured email addresses upon a password reset request from the sign-in page.

Before you begin

- Make sure that you are logged in to the VSP One File management software as security administrator (secadmin) and start Keycloak.
- Make sure that the security administrator (secadmin) user account is configured with an email address.

Procedure

1. Navigate to **Configure** > **Realm settings**.
2. In the **smu** page, click the **Email** tab and complete the following information:
   a. In the **From** box, enter the email address that the VSP One File management software should use to send emails.
   b. In the **Reply to** box, enter the email address that VSP One File management software should use to receive emails.
   c. In the **Host** box, enter the IP address or host name for the SMTP server.
   d. In the **Port** box, enter the port for the SMTP server. The default port number is 25.

e. Click **Enable SSL** to enable the SSL protocol for the SMTP server.

f. Click **Enable StartTLS** to enable the TLS protocol for the SMTP server.

g. (Optional) Set **Authentication** to on to enable authentication for the SMTP server, and then enter the login username and password to connect to the SMTP server.

h. Click **Test connection** to connect to the SMTP server.

   Testing the server connections sends a notification email to the security administrator.

3. Click **Save**.

Chapter 8: Configuring users and security

You can configure the VSP One File management software users and security as the security administrator (secadmin).

The VSP One File management software incorporates a set of predefined roles designed to manage user access to specific actions. For identity and access management, you can specify users in Keycloak.

Note: A user assigned to the security administrator (secadmin) role should not be assigned to any other role.

Configuring users

You can add users, user groups (groups), and assign user roles (realm roles or roles) to user groups in VSP One File management software using Keycloak.

A group can be assigned one or more roles, and users in a group inherit all roles assigned to that group. There are 10 preconfigured groups that inherit 10 preconfigured roles. For example, the administrator group inherits the administrator role. The preconfigured roles cannot be modified or deleted.

The following table shows the preconfigured user roles in Keycloak:

Role	Access level description
Administrator	Can perform all operations in File Administrator and System Administrator.
Administrator read-only	Has read-only access to File Administrator and System Administrator.
Backup and replication manager	Can perform the following operations in File Administrator: ▪ Manage NDMP backups of managed servers ▪ Manage file and object replication ▪ Manage data migration to cloud
Backup and replication manager read-only	Has read-only access to NDMP, replication services, and data migration.

Role	Access level description
File services manager	Can perform the following operations in File Administrator: ▪ Manage enterprise virtual servers (EVS) ▪ Migrate EVS ▪ Manage file systems ▪ Manage file migration ▪ Manage data migration to cloud ▪ Manage file service protocols such as FTP, iSCSI, NFS, and SMB.
File services manager read-only	Has read-only access to EVS, file systems, and file systems protocols.
Security administrator	Can perform all operations in Keycloak and System Administrator.
Security administrator read-only	Has read-only access to Keycloak and System Administrator.
Storage manager	Can perform the following tasks in File Administrator: ▪ Manage storage pools ▪ Manage system drives
Storage manager read-only	Has read-only access to storage drives and system pools.

In Keycloak, you can add users in two ways:

- Adding users locally (on page 26)
- Adding users using LDAP (on page 28)

The VSP One File management software ships with three preconfigured local users called admin, secadmin, and secadminro assigned with the role of administrator, security administrator, and security administrator read-only.

Note: You should sign-in at least once as User ID: `admin`, `secadmin`, and `secadminro` using the default Password: `nasadmin` to change the password for each user when prompted.

Adding users locally

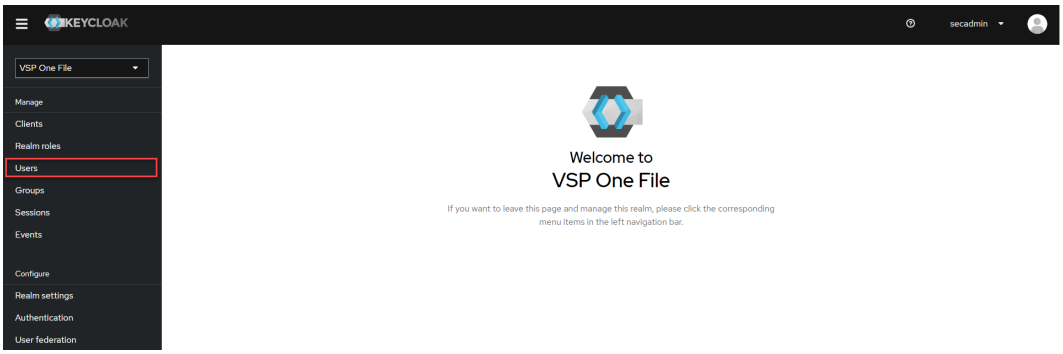
You can add users locally in VSP One File management software using Keycloak and assign them to a preconfigured role.

Before you begin

- Make sure that you are logged in to the VSP One File management software as security administrator (secadmin) and start Keycloak.
- Make sure that the user is assigned a valid email address.

Procedure

1. Navigate to **Manage** > **Users**.



2. In the **Users** page, click **Add user**.
3. In the **Create user** page, complete the following information:
   a. In the **Required user actions** list, choose one of the following options:
      - Select **Update Password** to reset the password to sign-in for the first time.
      - Select **Configure OTP** to configure multi-factor authentication to sign-in for the first time.
   b. Enter the username.

      A username can be a combination of letters (A-Z, a-z), numbers (0-9), and special characters.
   c. Enter the email address of the user that is valid and associated with an organization, and then set the **Email verified** toggle switch to **Yes**.
   d. (Optional) Enter the first name and last name of the user.
   e. To define the user access in the VSP One File management software, click **Join Groups**.
   f. In the **Select groups to join** page, select a group to assign one of the preconfigured roles to the user and then click **Join**.

      For example, to assign the user the role of a file service manager, select the File Services Managers group.
   g. Click **Create**.
4. In the **User details** page, select the **Credentials** tab, and then click **Set password** to configure the initial login credentials of the user.
5. In the **Set password for <username>** page, enter and confirm the user password.

   The password must be at least eight characters and must contain at least one, uppercase letter, number, and special character. For example, Password@123.
6. Set the **Temporary** toggle switch to **On** to make sure that the user is prompted to change the password at the first login.

7. Click **Save** and then send an email to the user with the login credentials.

Adding users using LDAP

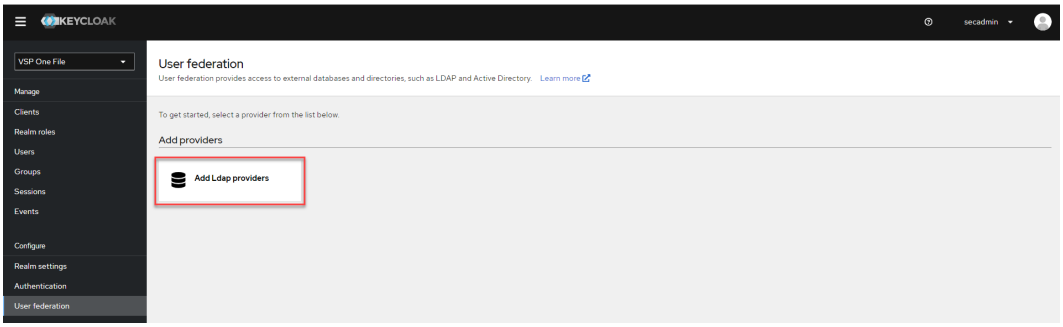
You can add users in VSP One File management software using Keycloak by connecting to an LDAP server. The LDAP server contains user groups which are mapped and synchronized to a local LDAP user group in Keycloak.

Before you begin

- Make sure that you are logged in to VSP One File management software as security administrator (secadmin) and start Keycloak.
- Make sure that a local LDAP group is created in Keycloak for synchronization with LDAP server groups.
- Make sure that you know the LDAP server vendor.

Procedure

1. Navigate to **Configure** > **User federation**.
2. In the **User federation** page, click **Add LDAP providers**.



3. In the **Add LDAP provider** page, complete the configuration to connect to the LDAP server, and then click **Save**. The configuration details are described in the Keycloak documentation.

   Make sure that you set the LDAP edit mode to **READ_ONLY** which restricts Keycloak to update user information like username and password on the LDAP server.

   If the LDAP server has large directory trees, do not import users locally as you can search users on Keycloak after connecting to the LDAP server.

4. In the LDAP configuration, click the **Mappers** tab, and then click **Add mapper**.
5. In the **Create new mapper** page, to map LDAP groups to Keycloak, enter the mapper name, select the **group-ldap-mapper**, and then complete the configuration to map the LDAP server to Keycloak, and then click **Save**. The mapping details are described in the Keycloak documentation.

   Make sure that you point the mapper path to the local Keycloak group folder, that the LDAP users appear inside the local Keycloak group after synchronization.

6. To synchronize the LDAP groups with the local LDAP group in Keycloak, select the **Action** list, and then click **Sync LDAP groups to Keycloak**.

   Keycloak notifies you when the synchronization between the LDAP server groups and the local LDAP group completes.
7. Navigate to **Manage** > **Groups**.
8. In the **Groups** page, click the local LDAP group.
9. In the LDAP group details page, click a sub-group.

   Groups in the LDAP server become sub-groups when synchronized to the local LDAP group in Keycloak.
10. In the sub-group details page, click the **Role Mapping** tab, and then assign a role to the sub-group.

    Users in the sub-group inherit the role assigned to the sub-group. The users can then use their LDAP credentials to login to the VSP One File management software.

Configuring security

You can configure security settings to control the hosts (clients with an IP address) that can access the VSP One File management software. You can also download logs to check user activity and troubleshoot login issues.

Configuring allowed hosts

Only hosts within the defined IP address range can communicate with the VSP One File management software and network devices.

Procedure

1. From the app switcher, select **System Administrator**.
2. Navigate to **Access** > **Security Options** > **Allowed Hosts**.
3. Set **Restrict Access to Allowed Hosts** toggle switch to on to add the **Allowed Hosts** to define individual IP addresses or a range of IP addresses that are allowed to access the VSP One File management software and devices on the network.

   Optionally, you can enter the allowed hosts using the IP address/netmask format, that is a netmask is added immediately following the IP address, and is separated from the IP address by a slash (`/`). The netmask can use the standard `#.#.#.#` format. For example, 192.0.2.0/255.255.255.0.

   Alternatively, you can enter the allowed hosts in network CIDR format (IP address/prefix), where the prefix is a simple number between 0 and 32. For example, `192.0.2.0/24`.

The value of specifying a prefix with an IP address is that you can allow access by a range of IP addresses with a single entry. For example, to allow access only by hosts having an IP address in the range 192.0.2.0 through 192.0.2.255, you could add the single entry `192.0.2.0/24` instead of entering each of the 256 entries individually.

Note: The netmask component does not directly specify the IP address at the end point of a range. For example, entering `192.0.2.0/192.0.2.255` does not allow VSP One File access for the hosts in the range `192.0.2.0` through `192.0.2.0`. Instead, to allow VSP One File access by all hosts in the range `192.0.2.0` through `192.0.2.255`, you would enter `192.0.2.1/255.255.255.0` or `192.0.2.0/24`.

The format for IPv6 address is: #:#:#:#:#:#:#:#, for example, fdca:f995:220a:480:1::a (which specifies a single host) or fdca:f995:220a:480:1::a/64 (which specifies a range of IP addresses in CIDR format).

4. Click **Apply**.

Downloading audit logs

You can download audit logs which contains information on user actions like successful logins, failed login attempts, password resets, user registrations, and administrative changes like client creation or user modification in the VSP One File management software.

Audit logs are used for troubleshooting login issues and maintaining an audit trail for accountability and detecting suspicious activity.

Procedure

1. From the app switcher, select **System Administrator**.
2. Navigate to **Access** > **Security Options** > **Audit Logs**.
3. In the **Audit Logs** pane, click **Download Audit Logs**.

   An text file is downloaded locally containing audit logs of VSP One File management software. An example of an audit log file format is `audit_events_XXX.txt`.

Configuring login banner

You can customize the security banner text by editing the text on the login banner page. A default security banner is provided as a sample security message to users.

Procedure

1. From the app switcher, select **System Administrator**.
2. Navigate to **Access** > **Security Options** > **Login Banner**.
3. Edit the security banner text by changing the text in the edit box. The security banner is plain without any formatting options.

   By default, the security banner is enabled.

   The login security banner is displayed on the VSP One File management software login screen. You cannot leave the banner empty.

4. Click **Apply**.
5. (Optional) To reset the login security banner to the default text, click **Reset to Default**.
6. Log out of the VSP One File management software and log back in to view the new banner text.

Configuring an SSL certificate

You can manage the security of the VSP One File management software domain by enabling the domain to use a secure protocol (https) with an SSL certificate.

An SSL certificate secures sensitive information using a public key. When the VSP One File management software receives the information, the software decrypts the information using a private key.

To configure an SSL certificate for the VSP One File management software, you must complete the following tasks:

- Create a private key for the SSL certificate, and then create a certificate signing request (CSR) to submit to a certificate authority (CA) to generate an SSL certificate.
- Upload the SSL certificate to the System Administrator.

Creating a certificate signing request

To generate an SSL certificate, you must create a CSR file that contains the fully qualified domain name (FQDN), organization name, location, and the public key. The CA validates this information and issues the SSL certificate. Before creating the CSR, you must create the private key.

Before you begin

Make sure that you have access to a Windows or Unix-based system with the OpenSSL toolkit installed. If the toolkit is not installed on the system, download and install it from https://openssl.org/.

Procedure

1. Open the command-line interface of the system.
2. To generate a private key, run the following command:

   ```
   openssl genpkey -algorithm RSA -out private.key -aes256
   ```

3. Enter and confirm a pass phrase for the private key.

   The pass phrase must be at least four characters. For example, P@ss123. Make sure to safely store the pass phrase.

4. To create a CSR, enter the following information:
   a. Run the following command:

      ```
      openssl req -new -key private.key -out request.csr
      ```

   b. When prompted, enter the following information:

i. **Country Name**: Enter the two-letter ISO code for the country. For example, for USA, enter US.
ii. **State or Province Name**: Enter the full name of the state or province where the organization is located. For example, California.
iii. **Locality Name**: Enter the full name of the city or locality where the organization is located. For example, Santa Clara.
iv. **Organization Name**: Enter the legal name of the organization. For example, Hitachi Vantara LLC.
v. **Organizational Unit Name**: Enter the name of department of the organization handling the request. For example, IT department.
vi. **Common Name**: Enter the FQDN of the website. For example, intranet.example.com.
vii. **Email Address**: Enter the email address of the requester.

5. Press the Enter key to skip the extra attribute, which is a challenge password that you can add to be sent with the CSR.
6. To verify the information in the CSR file, run the following command:

```
openssl req -text -noout -verify -in request.csr
```

7. Submit the CSR to one of the following CAs:
   - Public CA: Submit the CSR to a public CA if the organization has a special arrangement with the CA to issue certificates for private domains.
   - Private CA: Submit the CSR to the internal CA of the organization that issues certificates for internal servers and services.

Next steps

After the CA issues the SSL certificate in `.crt` or `.pem` format, upload the certificate using the System Administrator. See Uploading an SSL certificate (on page 32).

Uploading an SSL certificate

Upload an SSL certificate to the System Administrator to secure the VSP One File management software domain.

Before you begin

Make sure you have a public certificate file (`.crt`) or (`.pem`) and a private key file (`.key`) saved locally.

Procedure

1. From the app switcher, select **System Administrator**.
2. Navigate to **Access** > **Security Options** > **SSL Certificate**.
3. Upload the public certificate file and the private key file.
4. Click **Upload**.
5. Restart the browser to apply the SSL certificate.

Configuring web security options

You can select a protocol that your browser supports and enable or disable cipher suites using Web security options.

Procedure

1. From the app switcher, select **System Administrator**.
2. Navigate to **Access** > **Security Options** > **Web Security Options**.
3. Select the **HTTPS Minimum Protocol** list and choose the protocol that your browser supports.
4. To disable cipher suites, move enabled cipher suites from **Enabled Cipher Suites** list to **Disabled Cipher Suites** list.

   At least one cipher suite must be enabled. By default, all cipher suites are enabled.

   Note: Cipher Suite is a set of cryptographic algorithms. It uses keys to encrypt and decrypt messages sent between two devices.

   Take care before disabling cipher suites, because not all cipher suites are supported by all browsers. It is necessary that one protocol and one cipher suite remains enabled.

   Disabling multiple protocols or cipher suites might result in losing access to the VSP One File management software. A warning appears in your browser if this happens.
5. Click **Apply**.

Chapter 9: Setting up the VSP One File management software

After you have installed the VSP One File management software, use the first time setup wizard to configure the management software for use.

You perform the first time setup as an administrator.

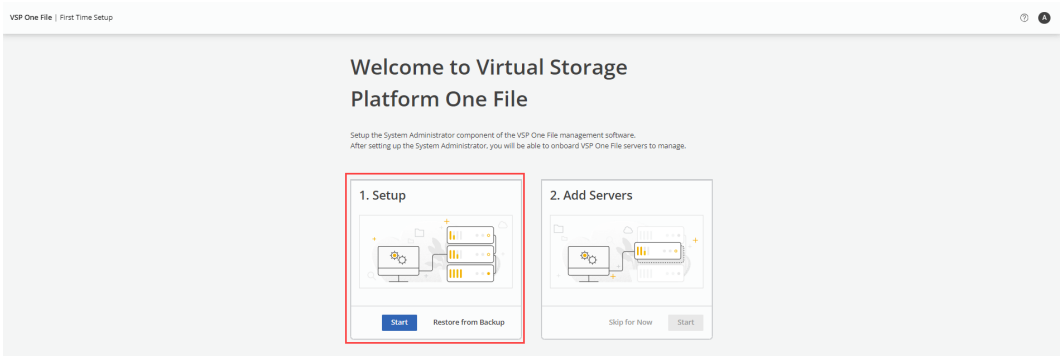
Setting up the VSP One File management software for the first time

Before you begin

- Make sure the VSP One File management software is installed.
- Obtain default admin login credentials from security administrator. Alternatively, you can login with the default credentials. User ID: `admin` and Password: `nasadmin`

Procedure

1. Log in to the VSP One File management software.
2. Change password when prompted. The password must contain uppercase and lowercase letters, numbers, and special characters.
3. In the **Setup** tile, click **Start** to open the setup wizard.



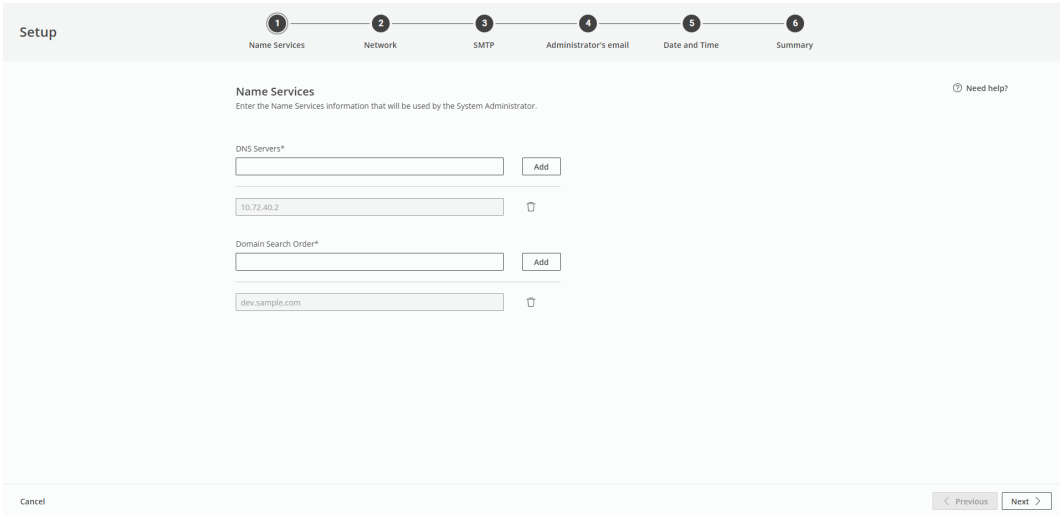
4. In the **Name Services** page, configure DNS server, and then click **Next**.
   - Domain Name System (DNS) is used for name resolution. In the **DNS Servers** field, enter a DNS server IP address and click **Add**. Repeat this step for each server that you want to add.

     Consider the following requirements when adding DNS servers:

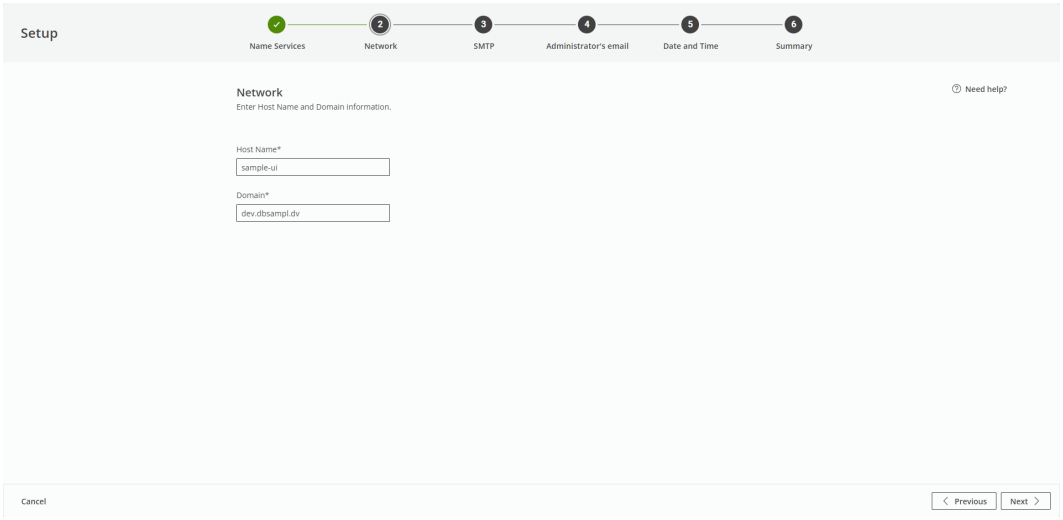
     - To add a DNS server by using an IPv6 address, IPv6 must be configured on the VSP One File server.
     - A DNS server can resolve host names to IPv4 or IPv6 addresses, whether it is connected to by IPv4 or IPv6.
     - If more than one DNS server is added, VSP One File searches for DNS servers in the order listed.
   - In the **Domain Search Order** field, enter a domain suffix (for example, `companyname.com`) to use as a search keyword and click **Add**.

     The DNS server searches for computer names using suffix order. For example, if the server contains the entries `uk.companyname.com` and `us.companyname.com`, a request for the IP address of a host named author generates a query for `author.uk.companyname.com` and then for `author.us.companyname.com`. However, the system does not search the parent domain `companyname.com`.

     Note: The suffix, combined with a computer's host name, makes up a fully qualified domain name.



5. In the **Network** page, enter the host name and domain name for the VSP One File server, and then click **Next**.

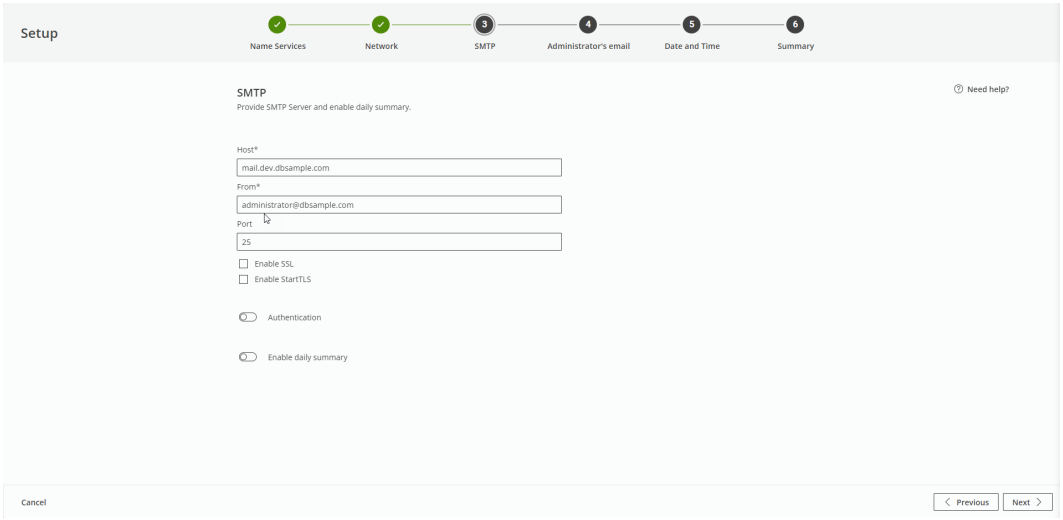


6. The VSP One File management software sends emails by using an SMTP server. In the **SMTP** page, complete the following information to configure the email settings, and then click **Next**.

   Note: If the security administrator (secadmin) configures the SMTP server from Keycloak, the SMTP server details will pre-populate on the **SMTP** page. You can change the SMTP configuration using this step.

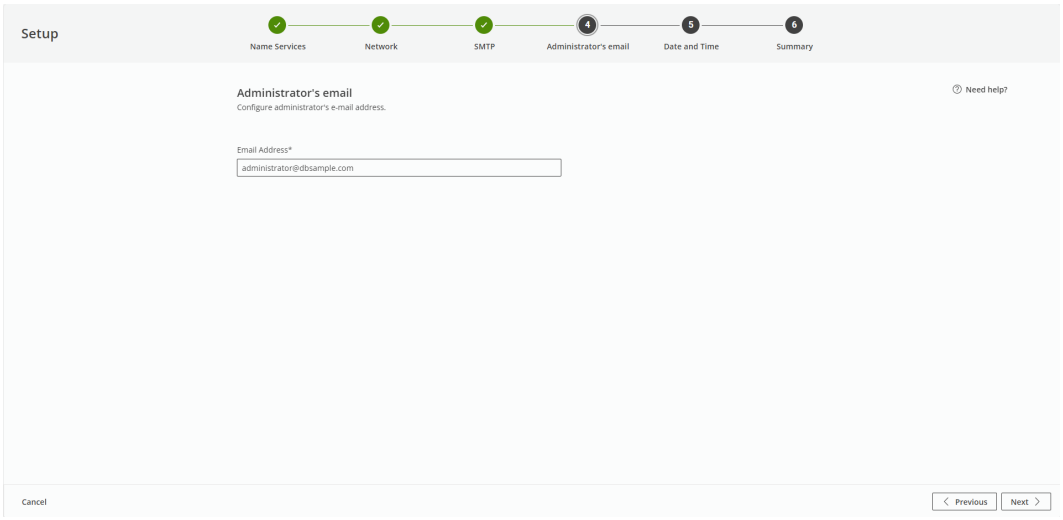
   - In the **Host** field, enter an IP address or host name for the SMTP server.

     If you specify an IPv6 address, VSP One File can use the SMTP server for email forwarding only if VSP One File is configured with an IPv6 address. Additionally, if the SMTP server is specified by host name and that host name resolves only to an IPv6 address, mail forwarding is possible only if an IPv6 DNS server is provided.
   - In the **From** field, enter the address for the email sender.
   - In the **Port** field, enter the port for the SMTP server. The default port number is 25.
   - Click **Enable SSL** to enable the SSL protocol for the SMTP server.
   - Click **StartTLS** to enable the TLS protocol for the SMTP server.
   - (Optional) Set **Authentication** to on to enable authentication for the SMTP server, and then enter a login username and password.
   - (Optional) Set **Enable Daily Summary** to on to get a daily status summary of the SMTP server. When you select this setting, VSP One File packages various logs, debugging, performance, and configuration settings for delivery to the specified recipient. Complete the following information for the email delivery:
     - In the **Add Recipients** field, enter a recipient email address, and then click **Add**. Repeat this step for each recipient that you want to add.
     - Click the **Send daily summary at** field, and select a time to send the summary each day.



7. In the **Administrator's Email** page, enter the email address for the VSP One File administrator to receive notifications, and then click **Next**.

> **Note:** The administrator email here is the pre-configured administrator user email that is shipped with VSP One File management software.



8. In the **Date and Time** page, specify whether you want to synchronize to an NTP server date and time or keep the default date and time by using one of the following options, and then click **Next**.

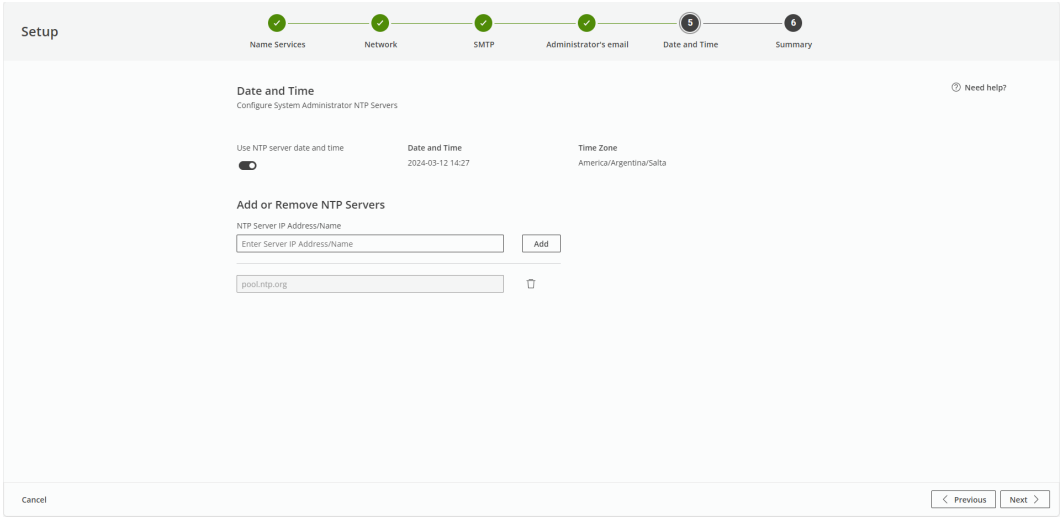
   - To synchronize the date and time to an NTP server, set **Use NTP server date and time** toggle switch to on.

     In the **NTP Server IP Address/Name** field, enter the IP address or host name that you want to use to synchronize the VSP One File server time, and then click **Add**. Repeat this step for each IP address or host name that you want to add.

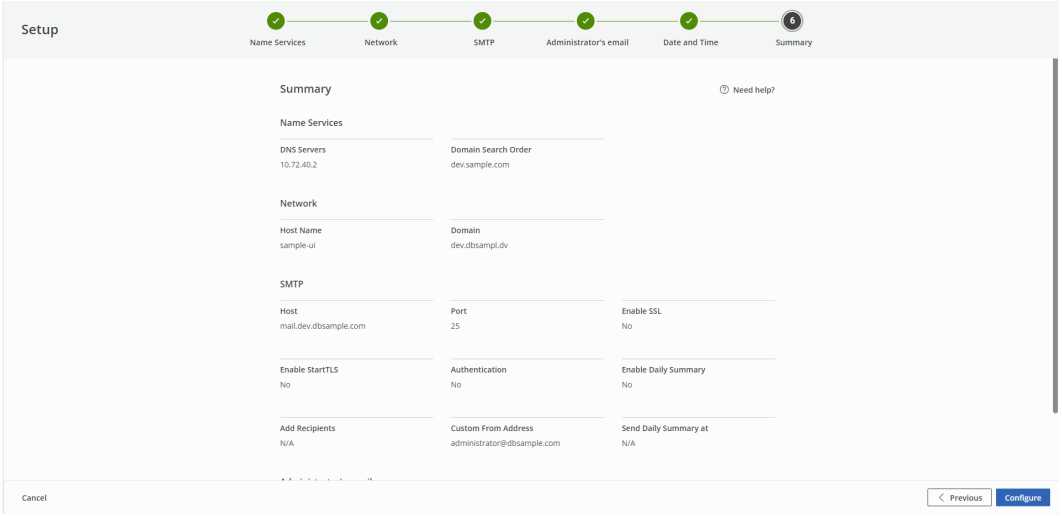
     > **Note:** If you specify an IPv6 address, VSP One File is able to synchronize only if it is configured with an IPv6 address. Additionally, if the NTP server is specified by host name and that host name resolves to an IPv6 address, synchronization is possible only if an IPv6 DNS server is provided.

     VSP One File qualifies and compares all listed NTP servers to determine and set the most accurate time. If several NTP servers are specified, VSP One File uses the first server in the list that it can contact.

   - To keep the default date, time, and timezone, set **Use NTP server date and time** toggle switch to off. Default is the VM server time in UTC.



9. In the **Summary** page, review the configuration settings, and then click **Configure**.



Result

The First Time Setup wizard completes the setup and displays the First Time Setup window suggesting that you add managed servers.

Next steps

After setting up the VSP One File management software, add servers. For more information, see Adding managed servers (on page 41).

Setting up by restoring from a backup file

During the first time setup, you can optionally replicate the VSP One File configuration from a local backup file. An example is replicating the configuration on the ESXi host to a standby ESXi host.

To restore from a backup file, the file must be created by using the VSP One File management software. Restore operations are not supported for backup files created by using the Hitachi NAS Platform System Management Unit (SMU).

Caution: Restoring overwrites the existing configuration. The restore process might take several minutes. When you restore from a backup, a system restart is required, which disrupts quorum device services.

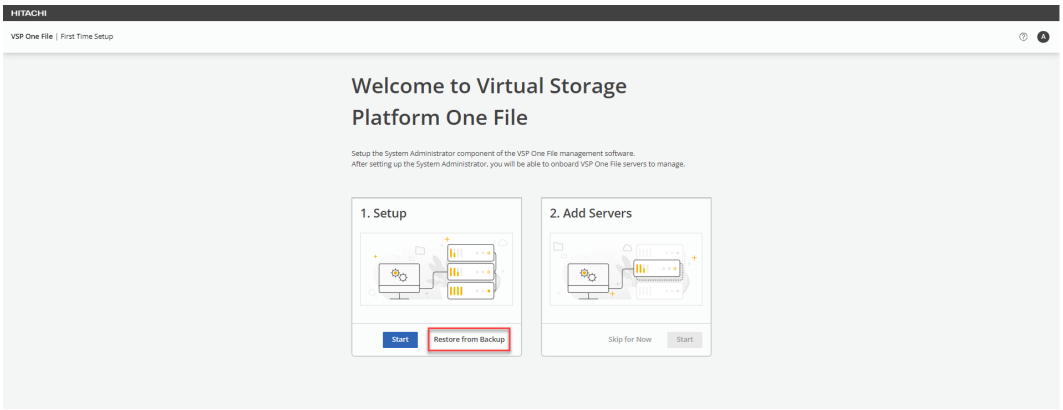
The restore process might affect the stability of clusters. Verify that clusters are in robust status before starting the restore process.

Before you begin

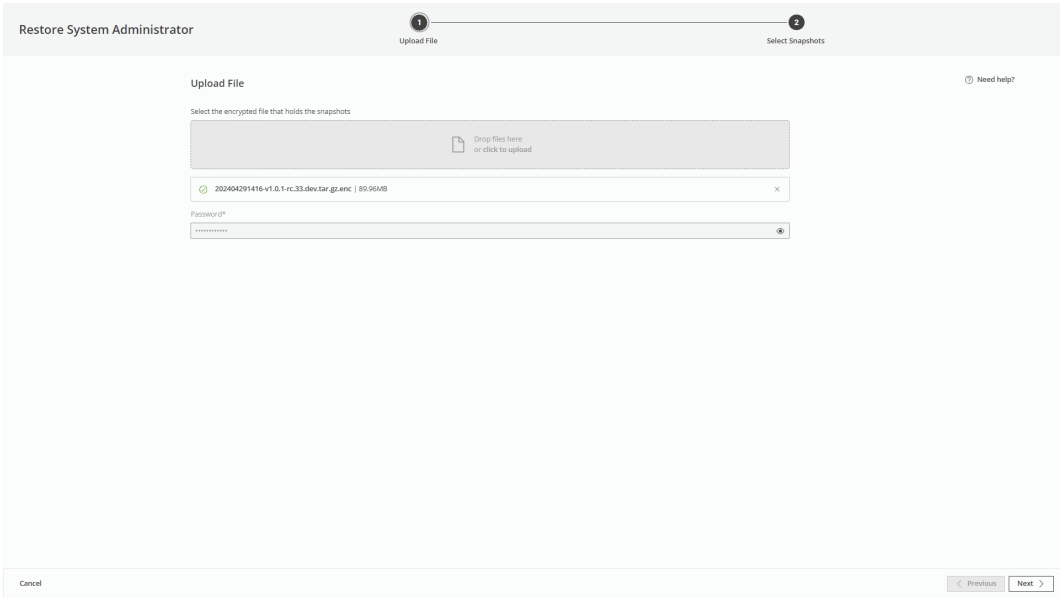
Ensure that you have the local backup file that you want to restore from and that you have the encryption password for the file. The password was assigned when the backup file was created as described in Backing up the VSP One File configuration (on page 52). Contact your administrator if you require assistance locating the password.

Procedure

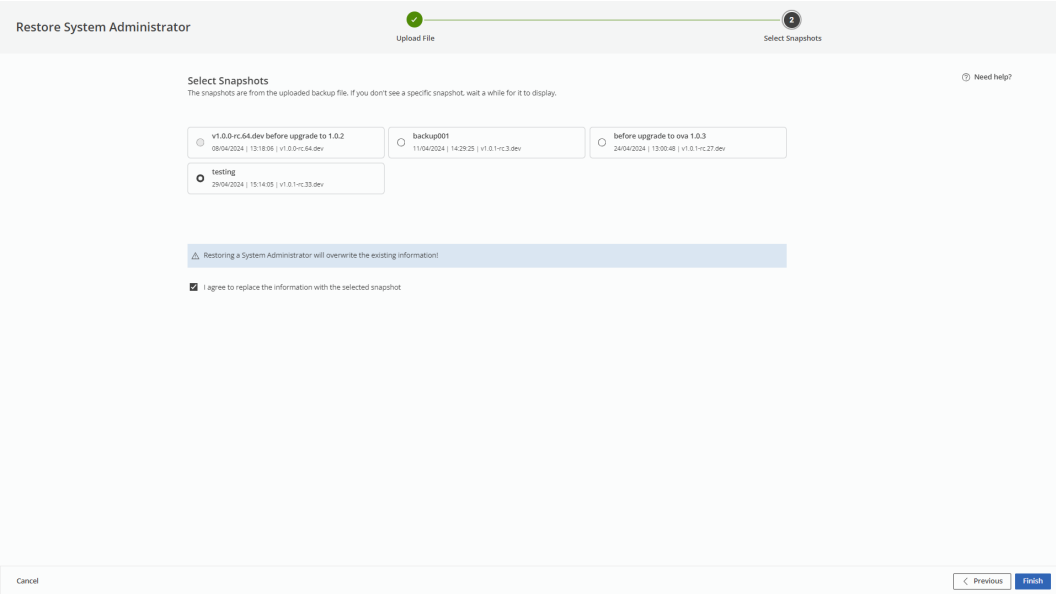
1. In the **Setup** tile, click **Restore from Backup** to open the restore wizard.



2. In the **Upload File** page, upload the local backup file, enter the encryption password for the file, and then click **Next**.



3. On the **Select Snapshots** page, select the snapshot that you want to restore from, accept the prompt to overwrite and replace the existing configuration, and then click **Finish**.



Restore in Progress is shown until the restore completes or fails and **Restore Completed** or **Restore Failed** is shown. You can click **View Log** to view log information for the restore process. The log information is useful for troubleshooting issues when the restore fails.

4. Click **Finish** to exit the wizard.

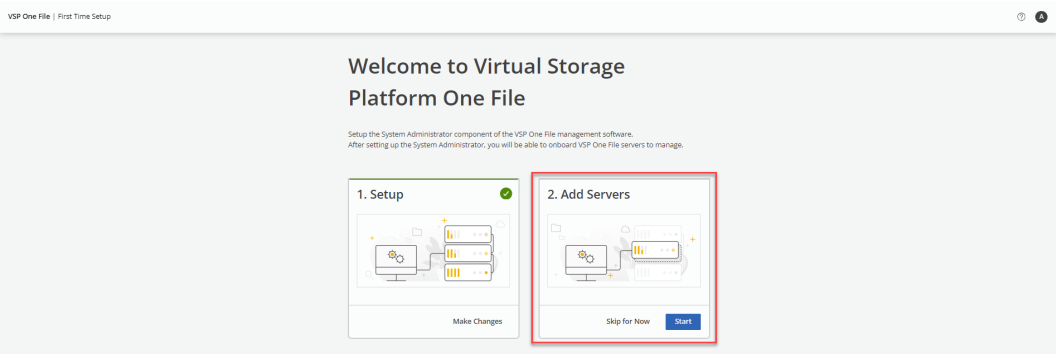
Adding managed servers

You can add multiple storage servers and storage clusters using the First Time Setup wizard.

Tip: After you add servers, you can manage servers as described in Managing servers (on page 45).

Procedure

1. In the **Add Servers** tile, click **Start**.



2. In the **Server Setup** page, enter the server IP address and user credential information, and then click **Establish Connection**.

Field	Description
Admin IP	Enter the IP address of the managed server. This should be the Administration Services IP address as used on the network.
Username	Enter the username used to log in to the managed server. For example, `supervisor`.
Password	Enter the password associated with the managed server username.

3. In the **Server Info** page, enter the server infomation, and then click **Next**.

Field	Description
Server Name	Enter a name for the managed server. The name can contain only alphanumeric characters and hyphens (-). The maximum number of characters is 13.
Location	Enter the location of the managed server.
Contact	Enter a contact number to use when there is an issue with the managed server.

Note: If you are adding a server that is already configured, skip the **Network**, **Email**, **Date and Time**, and **Install Licenses** pages in the wizard.

4. In the **DNS** page, enter the domain name and IP addresses of the DNS server, set the domain search order priority, set the name services ordering, set either LDAP or NIS mode. and then click **Next**.
   - A DNS server can be added by an IPv4 or IPv6 address (not by host name).
   - If a DNS server is to be added by an IPv6 address, IPv6 must be configured on the managed server.
   - A DNS server can resolve host names to IPv4 or IPv6 addresses whether it is connected to by IPv4 or IPv6.
   - If NIS mode is selected, enter the NIS domain name.

   Note: In **Domain Search Order**, you can list up to six DNS domains.

5. In the **SMTP** page, enter the SMTP server details and set up an email profile for receiving managed server status alerts, and then click **Next**.

Field	Description
Email Profile Name	Enter a name of email system that sends an alert on server status to the server administrators.
Send Summaries at hh:mm	Enter the time that the managed server sends out the daily summary status emails.
Severe	Select the frequency that the managed server sends out a severe alert.
Warning	Select the frequency that the managed server sends out a warning alert.
Information	Select the frequency that the managed server sends out any information emails to the server administrators.
Add Recipients	Add the email addresses of all the managed server administrators.

6. In the **NTP** page, enter the time, date, timezone, optionally NTP server name or IP address, and then click **Next**.
7. (Optional) In the **Set Passwords** page, change the **supervisor**, **manager**, and **root** user passwords, and then click **Next**.
8. In the **Install Licenses** page, verify the current cluster licenses of the managed server or add a new license key.

   Note: Obtain license keys from your Hitachi Vantara representative.

   a. To add a new license key, click **+ Add License Key**.
   b. In **Add License Key** page, add a license key or upload a locally saved license key from a file, and then click **Add**.
   c. Click **Next**.
9. In the **Node Type** page, choose one of the following node types, and then click **Next**.
   - For **Single Node**, continue with the steps in this topic.
   - For **Cluster Node**, complete the following information:
     a. Enter the cluster name, IP address and subnet mask of the cluster.
     b. Select a quorum device for the cluster.
     c. Select a node to add to the cluster. Alternatively, to add a node manually, click **+ Add Node Manually**. In the **Add Node Manually** dialog box, add the IP address, username, and password of the node, and then click **Add**.

10. In the **Summary** page, review the server configuration, and then click **Submit**.

    To add another managed server, click **Submit & add another**. The **Add Server** wizard completes the managed server configuration.

Next steps

Navigate to Managed Servers to view and manage the servers.

Chapter 10: Managing the VSP One File configuration

This module describes the tasks for maintaining the VSP One File configuration.

Managing servers

Storage and clusters that are administered by VSP One File are referred to as managed servers. You can add managed servers during the initial set up of the VSP One File management software by using the First Time Setup wizard and you can continue to add servers after the initial set up.

You can also modify and remove managed servers.

Adding a managed server

Procedure

1. From the app switcher, select **System Administrator**.
2. Navigate to **Managed Servers**.
3. In the **Managed Servers** pane, click **Add Server**.
4. In the **Server Setup** page, enter the server IP address and user credential information, and then click **Establish Connection**.

Field	Description
Admin IP	Enter the IP address of the managed server. This should be the Administration Services IP address as used on the network.
Username	Enter the username used to log in to the managed server. For example, `supervisor`.
Password	Enter the password associated with the managed server username.

5. In the **Server Info** page, enter the server infomation, and then click **Next**.

Field	Description
Server Name	Enter a name for the managed server. The name can contain only alphanumeric characters and hyphens (-). The maximum number of characters is 13.
Location	Enter the location of the managed server.
Contact	Enter a contact number to use when there is an issue with the managed server.

Note: If you are adding a server that is already configured, skip the **Network**, **Email**, **Date and Time**, and **Install Licenses** pages in the wizard.

6. In the **DNS** page, enter the domain name and IP addresses of the DNS server, set the domain search order priority, set the name services ordering, set either LDAP or NIS mode. and then click **Next**.
   - A DNS server can be added by an IPv4 or IPv6 address (not by host name).
   - If a DNS server is to be added by an IPv6 address, IPv6 must be configured on the managed server.
   - A DNS server can resolve host names to IPv4 or IPv6 addresses whether it is connected to by IPv4 or IPv6.
   - If NIS mode is selected, enter the NIS domain name.

   Note: In **Domain Search Order**, you can list up to six DNS domains.

7. In the **SMTP** page, enter the SMTP server details and set up an email profile for receiving managed server status alerts, and then click **Next**.

Field	Description
Email Profile Name	Enter a name of email system that sends an alert on server status to the server administrators.
Send Summaries at hh:mm	Enter the time that the managed server sends out the daily summary status emails.
Severe	Select the frequency that the managed server sends out a severe alert.
Warning	Select the frequency that the managed server sends out a warning alert.

Field	Description
Information	Select the frequency that the managed server sends out any information emails to the server administrators.
Add Recipients	Add the email addresses of all the managed server administrators.

8. In the **NTP** page, enter the time, date, timezone, optionally NTP server name or IP address, and then click **Next**.
9. (Optional) In the **Set Passwords** page, change the **supervisor**, **manager**, and **root** user passwords, and then click **Next**.
10. In the **Install Licenses** page, verify the current cluster licenses of the managed server or add a new license key.

    Note: Obtain license keys from your Hitachi Vantara representative.

    a. To add a new license key, click **+ Add License Key**.
    b. In **Add License Key** page, add a license key or upload a locally saved license key from a file, and then click **Add**.
    c. Click **Next**.
11. In the **Node Type** page, choose one of the following node types, and then click **Next**.
    - For **Single Node**, continue with the steps in this topic.
    - For **Cluster Node**, complete the following information:
      a. Enter the cluster name, IP address and subnet mask of the cluster.
      b. Select a quorum device for the cluster.
      c. Select a node to add to the cluster. Alternatively, to add a node manually, click **+ Add Node Manually**. In the **Add Node Manually** dialog box, add the IP address, username, and password of the node, and then click **Add**.
12. In the **Summary** page, review the server configuration, and then click **Submit**.
    To add another managed server, click **Submit & add another**. The **Add Server** wizard completes the managed server configuration.

Modifying a managed server

If the IP address, username, or password of a managed server has changed, you can update the information to maintain connection to the server.

Procedure

1. Navigate to **Managed Servers**.
2. In the **Managed Servers** pane, identify that server that you want to modify, and then click the edit icon.

3. Update the server IP address, username, or password.

   To retain the existing password, leave the **Password** box blank.
4. Click **Save Changes**.

Removing a managed server

Before you begin

Contact your system administrator before removing a managed server. When a server is removed, the following items are also removed:

- Replication policies and schedules.
- Data migration policies and schedules.
- The system monitor for the server.
- Racks managed by the server.

Procedure

1. Navigate to **Managed Servers**.
2. In the **Managed Servers** pane, select the server or servers that you want to remove, and then click **Remove**.
3. Click **Remove** to confirm.

Modifying the VSP One File management software network configuration

The network settings include the VSP One File management software host name, domain name, IPv4 address, and optional IPv6 address.

The VSP One File management software supports both IPv4 and IPv6 at the same time (dual-stack). IPv4 uses a 32-bit address and has an insufficient number of available addresses for global usage. IPv6 uses a 128-bit address that provides a much larger pool of addresses.

The network configuration settings are defined during the installation and initial set up of the VSP One File management software. You can change the settings at any time.

Caution: When network configuration changes, communication to quorum devices is disrupted until the VSP One File management software restarts.

Procedure

1. Navigate to **Configuration** > **Network**.
2. In the **System Configuration** section, enter the host name and the domain name for the VSP One File management software.

3. In the **IPv4 Configuration** section, enter the following information:
   - In the **IP Address** box, enter an IPv4 IP address for the VSP One File management software.
   - In the **Netmask** box, enter a netmask for the IP address. The netmask can be entered in #.#.#.# format. For example, 255.255.255.0.
   - In the **Gateway** box, enter the gateway IP address for the VSP One File management software.
   - **Current Addresses** shows any current static, SLAAC, and link-local addresses.
4. (Optional) In the **IPv6 Configuration** section, enter the following information:
   - Set the **IP Addresses** toggle switch to on to add an IPv6 address. You can use a static IP address or use stateless automatic configuration to provide the IP address.
     - In the **Static IP Address - CIDR Format** box, enter a static IP address in Classless Inter-Domain Routing (CIDR) format. You can enter an optional gateway in the **Gateway** box. If you leave the **Gateway** box blank, the VSP One File management software uses an advertised router as a gateway.
     - Select **Use stateless autoconfiguration (SLAAC)** to enable Stateless Address Auto-configuration (SLAAC) to automatically generate an IPv6 address. The address is generated from the prefixes contained in the router advertisements.
5. Click **Save Changes**.
6. Refresh the browser to use the new network settings.

Synchronizing the VSP One File management software with NTP server

You can synchronize the date, time and timezone of the VSP One File management software to a Network Time Protocol (NTP) server.

Procedure

1. Navigate to **Configuration** > **Date and Time**.

2. In the **Date and Time** pane, specify whether you want to synchronize to an NTP server date and time or keep the default date and time by using one of the following options:
   - To synchronize the date and time to an NTP server, set the **Use NTP server date and time** toggle switch to on.

     An NTP server can be specified by an IPv4 or IPv6 address or by a host name. When specified, VSP One File gets the current date and time from this NTP server and periodically checks with this NTP server to keep the clock accurate. If several NTP servers are specified, VSP One File uses the first one in the list that it can contact.

     Note: If an IPv6 address is specified, VSP One File is able to synchronize only if it is configured with an IPv6 address. Additionally, if the NTP server is specified by host name and that host name resolves to an IPv6 address, synchronization is possible only if an IPv6 DNS server is provided.

     For each NTP server, enter the IP address or name, and then click **Add**.

     To remove an NTP server, click the delete icon.
   - To keep the default date, time and timezone, set the **Use NTP server date and time** toggle switch to off. Default is the VM server time in UTC.
3. Click **Save Changes.**

Modifying the SMTP server settings

VSP One File receives and sends emails by using an SMTP server.

The SMTP server settings are configured during the initial set up of the VSP One File management software by using the First Time Setup wizard. You can change the settings at any time.

Procedure

1. Navigate to **Configuration** > **SMTP**.
2. In the **SMTP Settings** pane, complete the following information:
   - In the **Host** box, enter an IP address or host name.
   - In the **From** box, enter the address for the email sender.
   - In the **Port** box, enter the port for the SMTP server. The default port number is 25.
   - Click **Enable SSL** to enable the Secure Sockets Layer (SSL) protocol for the SMTP server.
   - Click **StartTLS** to enable the Transport Layer Security (TLS) protocol for the SMTP server.
3. (Optional) Set the **Authentication** toggle switch to on to enable authentication for the SMTP server, and then enter a login username and password.

4. (Optional) Set the **Enable Daily Summary** toggle switch to on to get a daily status summary of the server and complete the following information. When you select this setting, System Administrator packages up various logs, debugging, performance and configuration settings and emails it to the specified recipient:
   - In the **Add Recipients** box, enter a recipient email address, and then click **Add.**. Repeat this step for each recipient that you want to add.

     To remove a recipient, click the delete icon.
   - Click the **Send daily summary at** box, select a time to send the summary each day.
5. Click **Save Changes**.

Upgrading the VSP One File management software

You can upgrade the VSP One File management software by uploading a release file.

Before you begin

- Download the release file (`smu-install-<version>.tar.gz`) from the Hitachi Vantara Support Website.
- Back up the VSP One File configuration and download the backup to a safe location. See Backing up the VSP One File configuration (on page 52).
- Take a snapshot of the virtual machine on which the VSP One File management software is running.

Procedure

1. Navigate to **Configuration** > **Upgrade**.
2. In the **Upgrade** pane, upload the latest release file, and then click **Upgrade**.
3. Click **Upgrade** to confirm.

   Note: Make sure that you allow the upgrade without interruption.

Result

After the upgrade, you are returned to the log in page.

Backing up and restoring the VSP One File configuration

You should have a consistent backup routine for the VSP One File management software. Backups help to ensure that data is recoverable, whether must recover from a catastrophic event or simply restore to a previous configuration.

The backup process creates an initial full backup of the software configuration and then creates incremental snapshots that include only new or changed data. Creating incremental snapshots is faster and more efficient than completing a full backup.

You can run a backup immediately or schedule a backup.

Downloading and saving backup files

You can download backup files and save them to a safe location. If the system fails or is corrupted and you cannot access VSP One File, you must have a backup file to restore the software configuration. When you download a backup file, you must create an encrypted password that is required to restore the backup. You can save the password to a secure location such as a password manager.

A backup file contains the initial backup and all associated snapshots.

Restoring the software configuration

You can restore from a snapshot listed in System Administrator or restore from a backup file that was downloaded and saved. To restore from a backup file, you must have the encrypted password that was created during the download process.

To restore from a backup file or snapshot, the file or snapshot must be created in the current version of the VSP One File management software. A restore is not supported for backup files and snapshots created in previous versions.

Backing up the VSP One File configuration

A backup of the VSP One File management software creates an initial full backup of the software configuration and then creates incremental snapshots that include only new or changed data.

Procedure

1. Navigate to **Configuration** > **Backup**.
2. In the **Backup** pane, specify whether you want to backup now or schedule a backup for later:
   - To backup now, click **Backup Now** on the **Available Snapshots** tab. In the backup dialog box, enter a description for the backup (maximum of 250 characters), and then click **Initiate Backup**.

     When the backup is complete, the backup snapshot is listed on the **Available Snapshots** tab.
   - To schedule a backup, click the **Schedule Snapshots** tab, and then click **Schedule Snapshot**. In the schedule dialog box, set the schedule time and frequency, and then click **Schedule Snapshot**.

     The scheduled backup is listed on the **Scheduled Snapshots** tab.
3. (Optional) To download backup snapshots to save locally, click **Download Backup**.

   Important: Backup snapshots are encrypted and require an 8 to 32-character password to be provided that contains at least one uppercase letter, one lowercase letter, and one number. You should save the password to a secure location such as a password manager. You are prompted for the password when you restore snapshots from the backup file.

Restoring the VSP One File configuration

You can restore the VSP One File configuration from a local backup file or an available snapshot. To restore a backup file or snapshot, the file or snapshot must be created in the current version of the VSP One File management software. Restore operations are not supported for backup files and snapshots created in previous versions.

Caution: Restoring from a backup overwrites any existing configuration. A restore operation can take several minutes. Once the backup restoration has completed, a system restart is required for the restored configuration to take effect.

WARNING: Restarting the system disrupts quorum device services. To prevent loss of service in a clustered configuration while the reboot is performed, make sure that all managed clusters are in a robust state before restarting the system.

Before you begin

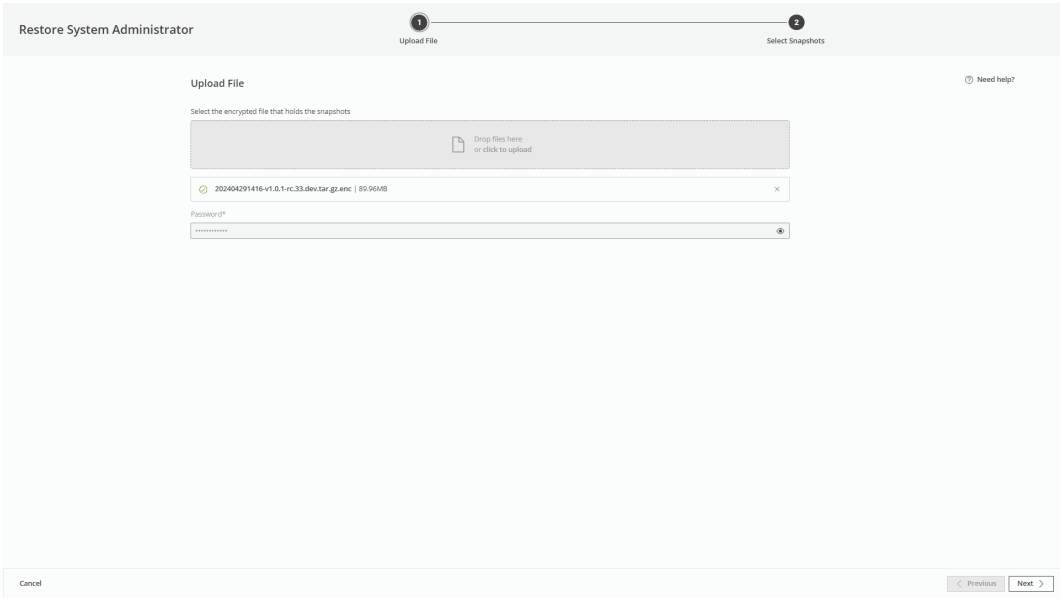
Ensure that you have the local backup file that you want to restore from and that you have the encryption password for the file. The password was assigned when the backup file was created as described in Backing up the VSP One File configuration (on page 52). Contact your administrator if you require assistance locating the password.

Procedure

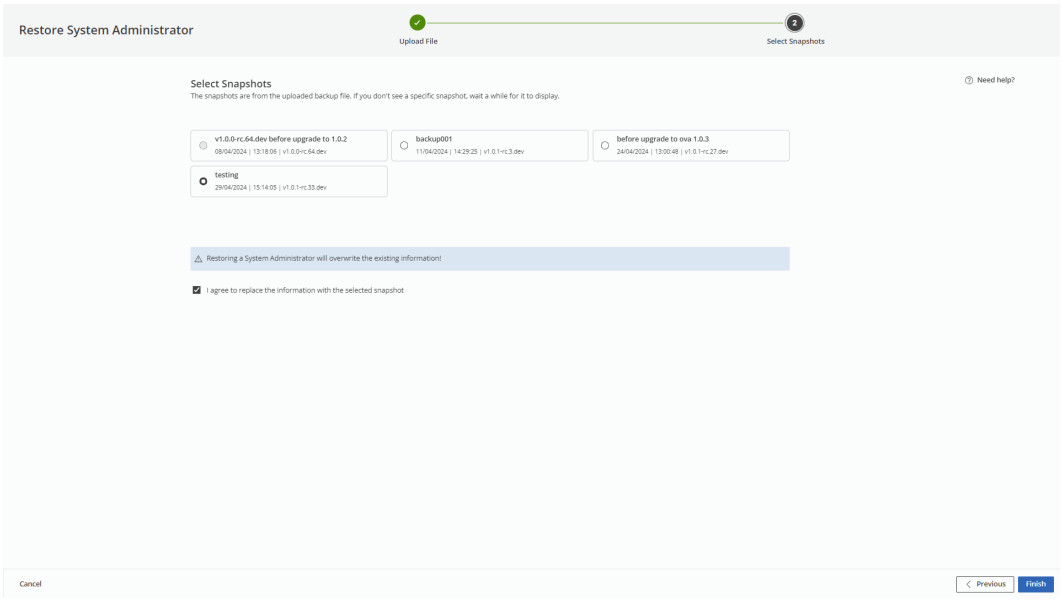
1. From the app switcher, select **System Administrator**.
2. Navigate to **Configuration** > **Restore**.

   Tip: The date, time, and status of the last restore is shown. Click **View log** to view additional information about the last restore process.
3. In the **Restore** window, specify whether you want to restore from a snapshot or restore from a backup file:
   - To restore from a snapshot listed in the **Restore** window, select the snapshot you want to restore, click **Restore**, and then click **Initiate restore**.

     You can select only snapshots created in the version of VSP One File that you are using. Snapshots created in other versions are shown, but not available. To verify the version, click the user icon, and then click **About**.
   - To restore from a backup file, click **Upload Snapshot** and enter the following information in the wizard:
     a. In the **Upload File** page, upload the local backup file, enter the encryption password for the file, and then click **Next**.



b. On the **Select Snapshots** page, select the snapshot that you want to restore from, accept the prompt to overwrite and replace the existing configuration, and then click **Finish**.



Restore in Progress is shown until the restore completes or fails and **Restore Completed** or **Restore Failed** is shown. You can click **View Log** to view log information for the restore process. The log information is useful for troubleshooting issues when the restore fails.

c. Click **Finish** to exit the wizard.

Modifying name services

Name services associate IP addresses with host names, which enables you to enter host names rather than IP addresses in the VSP One File management software. VSP One File supports the Domain Name System (DNS) for name resolution.

The name services are configured during the initial set up by using the First Time Setup wizard. You can change the settings at any time.

Procedure

1. Navigate to **Configuration** > **Name Services**.

   The server domain name is shown in the **DNS Domain** section.
2. In the **DNS Servers** box, enter a server IP address and click **Add**. Repeat this step for each server that you want to add.

   If more than one DNS server is added, the search is performed using the DNS servers in the order listed.

   To remove a DNS server, click the delete icon.
3. In the **Domain Search Order** box, enter a domain suffix (for example, `companyname.com`) to use as a search keyword and click **Add**.

   When searching for a computer name, the DNS server searches using suffix order. For example, if the server contains the entries `uk.companyname.com` and `us.companyname.com`, a request for the IP address of a host named author generates a query for `author.uk.companyname.com` and then for `author.us.companyname.com`. However, the system does not search the parent domain `companyname.com`.

   Note: The suffix, combined with a computer's host name, makes up a fully qualified domain name.

   To remove a DNS suffix, click the delete icon.
4. Click **Save Changes.**

Chapter 11: Upgrading the VSP One File management software

You can upgrade the VSP One File management software by uploading a release file.

Before you begin

- Download the release file (`smu-install-<version>.tar.gz`) from the Hitachi Vantara Support Website.
- Back up the VSP One File configuration and download the backup to a safe location. See Backing up the VSP One File configuration (on page 52).
- Take a snapshot of the virtual machine on which the VSP One File management software is running.

Procedure

1. Navigate to **Configuration** > **Upgrade**.
2. In the **Upgrade** pane, upload the latest release file, and then click **Upgrade**.
3. Click **Upgrade** to confirm.

> **Note:** Make sure that you allow the upgrade without interruption.

Result

After the upgrade, you are returned to the log in page.

Appendix A: Advanced features

The VMware vSphere ESXi provides advanced features to System Administrator.

Caution: Before you use any advanced features, verify that the system is configured correctly and that it can operate with advanced features installed.

Install VMware Tools® to make sure your system is configured correctly to run advance features.

VMware vSphere® High Availability features

VMware vSphere® High Availability (HA) monitors all virtualized servers and detects physical server and operating system failures. VMware High Availability can improve the availability of VSP One File and make file deployments more robust.

vSphere Fault Tolerance (FT) provides continuous availability for applications if a server fails.

The following are the HA and FT configuration options:

- **VMware vSphere vMotion®** and **Storage vMotion®**: Provide manual and automatic migration of compute and storage without service interruption. The three vMotion scenarios are:
  - **Host-only migration (with shared storage):** moves VM execution from one host to another.
  - **Storage-only migration (single host access to two storage pools):** moves a VM disk image from one storage pool to another storage pool.
  - **Host and storage migration:** combines both host and storage migration.

  The risk of losing quorum is none to minimal. However, vMotion does not protect against an ESXi host loss.
- **Cold standby:** In an ESXi HA cluster, if the ESXi host running VSP One File fails, a new instance of VSP One File starts on another ESXi host. The new instance uses the last updated disk image from the shared storage. Although recovery is fast, it requires starting the VM, which is not fast enough to prevent a quorum loss. If the VSP One File cluster is healthy, a HA failover does not affect its availability, but it does prevent access to the management software and the CLI while the new instance of starts.

  The risk of losing quorum is high to certain.
- **Hot standby:** With FT on, a the secondary VSP One File instance (on a different ESXi host) takes over immediately from a primary VSP One File if the primary fails. This requires a 10-Gbps FT logging network in addition to the normal network that connects the ESXi hosts and the VSP One File nodes. If VSP One File serves as a quorum device, the failover should be within the 5 second requirement before a quorum loss occurs. In this case, a HA failover can occur without affecting the File cluster, even if one of the file nodes is down.

  The risk of losing quorum is none to minimal.

In summary, HA provides a highly available VSP One File, but failovers can cause a short-term loss of quorum. FT provides a highly available VSP One File with a negligible chance of losing quorum.

Guidelines and requirements

Follow these guidelines when you use vSphere High Availability (HA) or Fault Tolerance (FT) to make sure that the system operates correctly.

- Verify that VMware Tools® is installed.
- Test that VMware vSphere® vMotion®, HA, or FT configurations are robust and operate correctly.
- To avoid creating a circular dependency, do not host VSP One File on the same file cluster for which VSP One File is providing quorum. A quorum loss could prevent access to the VSP One File disk image.
- Follow guidelines for CPU and memory allocations. Make sure that the VSP One File VM always has sufficient resources so that the quorum device is not paused or unresponsive for more than 5 seconds.
- Use 10 Gbps for the FT logging network. If you use less than 10 Gbps for the FT logging network, it negatively affects on the VSP One File performance.
- Use a larger ESXi license when required rather than limit the number of virtual CPUs. FT configurations allow a maximum of two or four virtual CPUs, depending on the ESXi license installed. If you have more than two or four managed entities, verify that operation is efficient with fewer than one virtual CPU per managed entity.
- Set up HA or FT configurations with the vSphere Web Client to receive error messages with more details.

For more information about vSphere High Availability, Fault Tolerance including features, license options, and pricing, visit: www.vmware.com.

Hitachi Vantara

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA

HitachiVantara.com/contact