## TABLES

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Typographical conventions used in this content</td>
</tr>
<tr>
<td>2</td>
<td>Revision history</td>
</tr>
<tr>
<td>3</td>
<td>Unisphere for VMAX Virtual Appliance VMware ESX Server requirements</td>
</tr>
</tbody>
</table>
As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your EMC representative if a product does not function properly or does not function as described in this document.

---

**Note**

This document was accurate at publication time. New versions of this document might be released on EMC Online Support (https://support.emc.com). Check to ensure that you are using the latest version of this document.

---

**Purpose**

This document describes how to install:

- Solutions Enabler virtual appliance
- Unisphere for VMAX virtual appliance
- VASA Provider virtual appliance

---

**Audience**

This document is intended for customers who are installing Virtual Appliance (vApp) Manager.

---

**Related documentation**

The following EMC publications provide additional information related to vApp Manager:

- *EMC Solutions Enabler Installation Guide*
- *EMC Unisphere for VMAX Installation Guide*
- *EMC Unisphere for VMAX Release Notes*
- *EMC Solutions Enabler Release Notes*
- *EMC VASA Provider Release Notes*

---

**Special notice conventions used in this document**

EMC uses the following conventions for special notices:

- **DANGER**
  Indicates a hazardous situation which, if not avoided, will result in death or serious injury.

- **WARNING**
  Indicates a hazardous situation which, if not avoided, could result in death or serious injury.
CAUTION
Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

NOTICE
Addresses practices not related to personal injury.

Note
Presents information that is important, but not hazard-related.

Typographical conventions
EMC uses the following type style conventions in this document:

<table>
<thead>
<tr>
<th><strong>Table 1</strong> Typographical conventions used in this content</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
</tr>
<tr>
<td><strong>Italic</strong></td>
</tr>
<tr>
<td><strong>Monospace</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Monospace italic</strong></td>
</tr>
<tr>
<td><strong>Monospace bold</strong></td>
</tr>
<tr>
<td>[ ]</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>{ }</td>
</tr>
<tr>
<td>...</td>
</tr>
</tbody>
</table>

Where to get help
EMC support, product, and licensing information can be obtained as follows:

Product information
EMC technical support, documentation, release notes, software updates, or information about EMC products can be obtained on the https://support.emc.com site (registration required).

Product information
For documentation, release notes, software updates, or information about EMC products, go to EMC Online Support at https://support.emc.com.
Product information
For documentation, release notes, software updates, or information about EMC products, go to EMC Online Support at https://support.emc.com or the CloudArray portal at https://www.cloudarray.com.

Technical support
To open a service request through the https://support.emc.com site, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or to answer any questions about your account.

Technical support
EMC offers a variety of support options.
- Support by Product — EMC offers consolidated, product-specific information on the Web at: https://support.EMC.com/products
  The Support by Product web pages offer quick links to Documentation, White Papers, Advisories (such as frequently used Knowledgebase articles), and Downloads, as well as more dynamic content, such as presentations, discussion, relevant Customer Support Forum entries, and a link to EMC Live Chat.
- EMC Live Chat — Open a Chat or instant message session with an EMC Support Engineer.

Technical support
For technical support, go to EMC Online Support https://support.emc.com and click Service Center. To open a service request, you must have a valid support agreement. Please contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

eLicensing support
To activate your entitlements and obtain your VMAX license files, visit the Service Center on https://support.EMC.com, as directed on your License Authorization Code (LAC) letter emailed to you.
- For help with missing or incorrect entitlements after activation (that is, expected functionality remains unavailable because it is not licensed), contact your EMC Account Representative or Authorized Reseller.
- For help with any errors applying license files through Solutions Enabler, contact the EMC Customer Support Center.
- If you are missing a LAC letter, or require further instructions on activating your licenses through the Online Support site, contact EMC’s worldwide Licensing team at licensing@emc.com or call:
  - North America, Latin America, APJK, Australia, New Zealand: SVC4EMC (800-782-4362) and follow the voice prompts.
  - EMEA: +353 (0) 21 4879862 and follow the voice prompts.

EMC SolVe Desktop
Provides links to documentation, procedures for common tasks, and connectivity information for 2-site and 3-site SRDF configurations. To download the SolVe Desktop tool, go to EMC Online Support at https://support.EMC.com and search for SolVe Desktop. Download the SolVe Desktop and load the VMAX All Flash, VMAX3 Family, VMAX, and DMX procedure generator.
Note
You need to authenticate (authorize) your SolVe Desktop. After it is installed, familiarize yourself with the information under Help tab.

Documentation within the Symmetrix Procedure Generator
The following EMC procedural documentation is available in the Symmetrix Procedure Generator.
The following EMC procedural documentation is available in the Symmetrix Procedure Generator.
For information regarding the Symmetrix Procedure Generator, see: http://www.corkc4.isus.emc.com/wiki/index.php/Symmetrix_Procedure_Generator

- Pre-Hardware Install Checklist
- Post-Hardware Install Checklist

Your comments
Your suggestions help us improve the accuracy, organization, and overall quality of the documentation. Send your comments and feedback to: VMAXContentFeedback@emc.com
The following table lists the revision history of this document.

**Table 2 Revision history**

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>September 23, 2016</td>
<td>First release of EMC Virtual Appliance Manager Installation Guide.</td>
</tr>
</tbody>
</table>
This chapter provides an overview of the Virtual Appliance Installation Guide. Topics include:

- Overview
Virtual Appliance (vApp) Manager provides the ability to manage and configure your storage environment. vApp Manager supports:

- Solutions Enabler
- Unisphere for VMAX
- VASA Provider
- Guest OS
- Embedded Management

This guide provides installation information for Solutions Enabler, Unisphere for VMAX, and VASA Provider Virtual Appliance instances. The Guest OS and Embedded Management Virtual Appliances are pre-installed at the factory.
CHAPTER 2

Installing the Solutions Enabler Virtual Appliance

This chapter explains how to install the Solutions Enabler Virtual Appliance in a VMware infrastructure environment. Topics include:

- Introduction .......................................................................................................... 16
- Before you begin ................................................................................................... 17
- Installing the virtual appliance directly to the ESX Server ....................................... 17
- Installing the virtual appliance through a vCenter Server ....................................... 20
- Installing the virtual appliance using OVFTOOL ...................................................... 21
- Launching vApp Manager ...................................................................................... 23
- Updating the Solutions Enabler Virtual Appliance .................................................. 23
- Deleting the Solutions Enabler Virtual Appliance ................................................... 24
Introduction

The Solutions Enabler Virtual Appliance is a VMware ESX server virtual machine that provides all the components you need to manage your storage environment using the storsrvd daemon and Solutions Enabler network client access. These include:

- EMC Solutions Enabler V8.3 (solely intended as a SYMAPI server for Solutions Enabler client access)
- Linux OS (SUSE 11 SP3 JeOS)
- SMI-S Provider V8.3

In addition, the Solutions Enabler Virtual Appliance includes a browser-based console called EMC vApp Manager for Solutions Enabler to configure your storage environment. vApp Manager enables you to perform the following configuration tasks:

- Monitor the application status
- Start and stop selected daemons
- Download persistent data
- Configure the nethost file (required for client access)
- Discover storage arrays
- Modify options and daemon options
- Add array-based and host-based license keys
- Run a limited set of Solutions Enabler CLI commands
- Configure ESX host and gatekeeper devices
- Launch Unisphere for VMAX (available only in Unisphere versions of the appliance console)
- Configure iSCSI initiator and map iSCSI gatekeeper devices
- Configure additional NIC card (optional)
- Download SYMAPI debug logs
- Import CA signed certificate for web browser
- Import Custom certificate for storsrvd daemon
- Check disk usage
- Restart appliance
- Configure symavoid entries
- Load array-based eLicenses
- Enable SSH
- Configure LDAP
- Manager users
- Reset hostname
- Update etc/hosts

For information on using vApp Manager, refer to its online help.

Root login is not supported on the SUSE 11 virtual machine.
Before you begin

Before you begin to install the Solutions Enabler Virtual Appliance, be sure to complete the tasks listed in this section:

Procedure

1. Verify that you are installing the latest version of the appliance by checking EMC Online Support for updates.
2. Verify that the client is running:
   - VMware vSphere Client
   - Any of the following browsers with cookies and JavaScript enabled:
     - Internet Explorer 9.0 through 11.0 (Desktop only)
     - Firefox 30 or later
     - Chrome 21.0.1180 or later
   Browsers should have Flash Player 11.2 plug-in installed. If your browser has an older version of Flash Player, you will be prompted to download the latest version when you start the web console.
3. Verify that the VMware ESX Server meets the following minimum requirements:
   - Version 4.0 or later
   - Dual disk. 16 GB of disk space and another 5 GB (expandable) disk space
   - 2GB memory
   - 1 CPU

Installing the virtual appliance directly to the ESX Server

This section describes how to install the Solutions Enabler Virtual Appliance directly to the ESX Server.

Note

When deploying the Virtual Appliance using command line via OVF, or while adding an ESX server in vApp Manager, make sure the ESX name is specified with the exact case as it is registered in the DNS otherwise, the attempted operation will fail.

Step 1: Import the virtual appliance

To import the virtual appliance:

Procedure

1. Download the OVF archive file (*.ova) containing the installation program from EMC Online Support to a temporary directory.
2. Start the vSphere Client and log in to the ESX Server on which you will be installing the appliance.
3. Click Ignore in the security warning message.
4. From the File menu, select Deploy OVF Template.
5. Browse to the OVF archive file, located in the temporary directory you created earlier. Select the OVF archive file with the suffix `vappxxx_xxx_OVF10.ova`.

6. Click Next.

7. On the Details page, verify the details about the appliance and click Next.

8. On the End User License Agreement page, select Accept all license agreements and click Next.

9. On the Name and Location page, specify a name for the appliance and click Next.

10. If a resource pool is available, the Resource Pool page displays. Select the resource pool of your choice and click Next. Otherwise, the Resource Pool page is skipped.

11. On the Datastore page, select the datastore of your choice and click Next.

12. On the Disk Format page, select the format in which to store the virtual machine's virtual disks and click Next.

13. On the Network Mapping page, map the source network to the appropriate destination network.

14. On the Ready to Complete page, verify the information and click Finish.

15. In the Completed Successfully message, click Close.


### Step 2: Select gatekeepers

Present uniquely defined gatekeepers by way of raw device mappings (RDM). For instructions, refer to the appropriate VMware documentation.

Solutions Enabler manages storage arrays through gatekeeper devices mapped to the virtual appliance as RDM pass-through devices. The management is done through EMC proprietary commands using SCSI 3B/3C write/read commands. For every call, a WRITE command is issued to send the request, and then a READ command to get the results.

---

**Note**

Gatekeepers can be added using vApp Manager. For ESX V4.0 and earlier, vApp Manager does not allow more than 14 gatekeeper volumes to be added to the Virtual Appliance. Attempting to add more than 14 gatekeepers returns an error message. For detailed information, refer to vApp Manager online help.

---

Continue with Step 3: Power on and configure the Virtual Appliance on page 18 below.

### Step 3: Power on and configure the Virtual Appliance

To power on and configure the Virtual Appliance:

**Procedure**

2. Click the Console tab and watch as the appliance starts up.
3. At the following prompts, enter static IP configuration information:

   Please select your static network configuration.
   For IPv4: Enter 1
   For IPv6: Enter 2
   Enter your choice [1]/2:

   Please enter static IP configuration:
• IP Address [ ]:
  Type the address assigned to the appliance, and then type y to continue with the configuration.

  **Note**
  The virtual appliance uses this IP address to query the DNS Server and get its hostname. Therefore, you must ensure that the IP address has a hostname mapping in the DNS Server.

• Netmask [ ]:
  Type the mask of the network on which the appliance will be running, and then type y to continue with the configuration.

• Gateway [ ]:
  Type the gateway address to the network on which the appliance will be running, and then type y to continue with the configuration.

• DNS1 [ ]:
  Type the first DNS server address, and then type y to continue with the configuration.

• DNS2 [ ]:
  Type the second DNS server address, and then type y to continue with the configuration.

• Is a proxy server necessary to reach the Internet? y/n [n]:
  A [y]es response enables you to specify the IP address of the proxy server and the port.

The network is configured at this point.

4. At the following prompt, specify whether you want to set the time zone:

   Do you want to set the time zone? y/[n] :

   A [n]o response continues the configuration. If you select this option, you can use the appliance console to specify the time zone at a later time.

   A [y]es response produces the following series of prompts that will enable you to set the time zone:

   • Please select a continent or ocean
     Type the number that corresponds to the time zone location and press Enter.

   • Please select a country
     Type the number that corresponds to the country-specific time zone you want to set and press Enter.

   • Please select one of the following time zone regions
     Type the number that corresponds to regional time zone you want to set and press Enter.

   The time zone is now set.

5. At the following prompt, specify whether you want to enter the host ESX Server information:

   Do you want to set the host ESX Server y/[n]? :
Installing the Solutions Enabler Virtual Appliance

6. Continue with Launching vApp Manager on page 23.

Installing the virtual appliance through a vCenter Server

This section describes how to install the Solutions Enabler Virtual Appliance through a vCenter Server 4.0 and later.

Step 1: Import and configure the virtual appliance

To import and configure the virtual appliance:

Procedure

1. Download the OVF archive file (*.ova) containing the installation program from EMC Online Support to a temporary directory.
2. Start the vSphere Client and log in to the vCenter Infrastructure Server through which you will be installing the virtual appliance.
3. Click Ignore in the security warning message.
4. From the navigation tree, select the ESX Server on which you will be installing the virtual appliance.
5. From the File menu, select Deploy OVF Template.
6. Browse to the OVF archive file, located in the temporary directory you created earlier. Select the OVF archive file with the suffix *vapp_OVF10.ova.
7. Click Next.
8. On the Details page, verify the details about the appliance and click Next.
9. On the End User License Agreement page, select Accept all license agreements and click Next.
10. On the Name and Location page, specify a name for the appliance and click Next. It is recommended that you name the appliance with the same fully qualified hostname of the virtual appliance.
11. Select the host/cluster to run the virtual appliance.
12. If a resource pool is available, the Resource Pool page displays. Select the resource pool of your choice and click Next. Otherwise, the Resource Pool page is skipped.
13. On the Datastore page, select the datastore of your choice and click Next.
14. On the Network Mapping page, map the source network to the appropriate destination network.
15. Customize the software solution for this installation by doing the following:
   a. Provide valid values for the following OVF properties:
- IP Address
- Netmask
- Gateway
- DNS Server 1
- DNS Server 2

**Note**
The virtual appliance uses this IP address to query the DNS Server and get its hostname. Therefore, you must ensure that the IP address has a hostname mapping in the DNS Server.

b. Optionally, provide/select valid values for the following OVF properties:

- Proxy Server: Enter the IP address of the proxy server and port. For example: `ProxyServer-IP:Port`
- ESX Server Name: Enter the fully qualified ESX Server hostname.
- ESX Server Password: Enter the ESX Server password in base64 encryption format.

16. On the **Ready to Complete** page, verify the information and click **Finish**.
17. In the Completed Successfully message, click **Close**.
18. Continue with **Step 2: Select gatekeepers on page 21** next.

**Step 2: Select gatekeepers**

**Procedure**

1. Select gatekeepers as described in **Step 2: Select gatekeepers on page 18**.
   
   You can configure the virtual appliance to add two gatekeeper devices per storage array when it firsts boots up. For instructions, refer to **Step 10 on page 20**.

2. Continue with **Step 3: Power on the virtual appliance on page 21** next.

**Step 3: Power on the virtual appliance**

To power on and configure the Virtual Appliance:

**Procedure**

1. On the **Summary** page of the Virtual Infrastructure Client, click **Power On**.
2. Click the **Console** tab and watch as the appliance starts up.

   A Welcome screen appears. You have now finished installing the Solutions Enabler Virtual Appliance.

3. Continue with **Launching vApp Manager on page 23**.

**Installing the virtual appliance using OVFTOOL**

Solutions Enabler Virtual Appliance can be installed through command line from any Linux host. This section how to install the virtual appliance using OVFTOOL.

To install Solutions Enabler Virtual Appliance using OVFTOOL, the following are required:
Installing the Solutions Enabler Virtual Appliance

- vCenter Server 4.0 and above.
- ESX Server 4.0 and above managed by vCenter Server 4.x.
- OVFTOOL 1.0 and above.

**Note**
Please refer to the appropriate documentation for installing vCenter Server and VMware ovftool.

Here is a brief description of the steps on how to install the virtual appliance using OVFTOOL:

1. Install and Setup the vCenter Server.
2. Add the ESX Server to the vCenter Server datacenter.
3. Install VMware OVFTOOL on a Linux host.
4. Move the Solutions Enabler Virtual Appliance kit to the above host.
5. Run the ovftool command with necessary command line switches. For more information on using the command, refer to Using OVFTOOL on page 22.
6. The Solutions Enabler Virtual Appliance is installed and powered on automatically.
7. Continue with Launching vApp Manager on page 23.

**Using OVFTOOL**

OVFTOOL has the following syntax:

```bash
/usr/bin/ovftool --acceptAllEulas --overwrite --powerOffTarget
--powerOn --prop:ipAddress=<IP-ADDRESS> --prop:netmask=<NETMASK>
--prop:gateway=<GATEWAY> --prop:dns1=<DNS1> --prop:dns2=<DNS2>
--prop:timezone=<TIMEZONE> --prop:esxServer=<ESX-SERVER>
--prop:encrRootPassword=<ROOT-PASSWORD> --name=<VM-DISPLAYNAME>
--datastore=<DATASTORE> --net:Network\ 1=<VM Network Port Group>
--net:Network\ 2=<VM Network Port Group> <OVA-FILE>
v://Administrator:<vCenter-admin-passwd>@<vCenter-Server>/<DataCenter-Name>/host/<esx-server-name>
```

Where:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP-ADDRESS&gt;</td>
<td>IP Address of the Virtual Appliance.</td>
</tr>
<tr>
<td>&lt;NETMASK&gt;</td>
<td>Netmask of the Virtual Appliance.</td>
</tr>
<tr>
<td>&lt;GATEWAY&gt;</td>
<td>Gateway.</td>
</tr>
<tr>
<td>&lt;DNS1&gt;</td>
<td>IP of DNS Server1.</td>
</tr>
<tr>
<td>&lt;DNS2&gt;</td>
<td>IP of DNS Server2.</td>
</tr>
<tr>
<td>&lt;TIMEZONE&gt;</td>
<td>Time Zone setting. (Optional)</td>
</tr>
<tr>
<td>&lt;ESX-SERVER&gt;</td>
<td>Fully qualified hostname of ESX server. (Optional)</td>
</tr>
<tr>
<td>&lt;ROOT-PASSWORD&gt;</td>
<td>Root password of ESX Server in base64 encrypted format. (Optional)</td>
</tr>
<tr>
<td>&lt;VM-DISPLAYNAME&gt;</td>
<td>VM Displayname. To automatically add gatekeeper devices during virtual appliance boot, VM Displayname to be same as fully qualified hostname of Virtual Appliance.</td>
</tr>
</tbody>
</table>
Launching vApp Manager

Once the vApp is deployed, follow the steps below to launch vApp Manager:

Procedure
1. Type one of the following URLs in a browser:

   https://appliance_IP:5480

   or

   https://appliance_host_name:5480

2. On the log in panel, type seconf for both the User and Password, and then click Login.

   Note
   You are required to change your password from vApp Manager on first login. vApp Manager can also be configured to use LDAP for user authentication. For more information on that, refer to the vApp Manager online help.

3. vApp Manager displays. For information on using vApp Manager, refer to its online help.

Updating the Solutions Enabler Virtual Appliance

Periodically, EMC will release security patches and hot-fixes for the Solutions Enabler Virtual Appliance. These patches and fixes are available on EMC Online Support in ISO images.

Updating from an ISO image

This procedure explains how to upgrade the virtual appliance to V8.3.

To update an existing Virtual Appliance from an ISO image:

Procedure
1. Upload the ISO image into the ESX Server using the VI client:
   a. Login to the ESX Server using the VI client.
b. Select the ESX Server on the left panel.

c. Select the **Configuration** tab on the right panel.

d. Select Hardware, Storage to list the datastores connected to the ESX Server.

e. Right-click the datastore and select **Browse Datastore**.

The **Datastore Browser** window displays.

f. Upload the appliance update ISO file.

g. Exit the dialog.

2. Mount the ISO image on the virtual appliance CD drive:

   a. Right-click the virtual appliance and select **Edit Settings**.

   b. On the **Hardware** tab, select **CD/DVD Drive 1**.

   c. In the right panel, select **Datastore ISO File**, and click **Browse** to locate the ISO image in the datastore.

   d. Select **Device Status**, **Connected**.

   e. Click **OK** to exit the dialog box.

3. Update the appliance:

   a. On the **Console** tab, go to the virtual appliance console.

   b. Use the Move Up/Down keys and select **Appliance Update**.

   c. Press **Enter** to perform the update.

   The update will take approximately 10 minutes, after which the screen will return to the main console.

   ________________

   **Note**

   Use the welcome screens of the vApp and the vApp Manager to confirm your virtual appliance has been updated correctly.

______________

**Deleting the Solutions Enabler Virtual Appliance**

To delete the Solutions Enabler Virtual Appliance:

**Procedure**

1. In the vApp Manager interface, backup the persistent data.

2. In the VMware management interface, power down the appliance.

3. Right-click on the appliance and select **Delete from Disk**.

4. Click **Yes** in the confirmation message.
CHAPTER 3

Installing the Unisphere for VMAX Virtual Appliance

This chapter explains how to install the Unisphere for VMAX Virtual Appliance in a VMware infrastructure environment. Topics include:

- Introduction ..................................................................................................................... 26
- Before you begin ............................................................................................................. 27
- Installing the virtual appliance directly on the ESX Server ........................................ 27
- Installing the virtual appliance through a vCenter Server ......................................... 33
- Installing the virtual appliance using OVFTOOL ....................................................... 35
- Launching Unisphere or the vApp Manager ................................................................. 38
- Registering the VASA Provider with vSphere ............................................................. 39
- Upgrading the Unisphere for VMAX Virtual Appliance using an ISO image .............. 40
- Re-configuring the virtual appliance IP address ......................................................... 42
- Deleting the Unisphere for VMAX Virtual Appliance ............................................... 43
- Backing up and restoring the performance database ................................................ 44
- Installing licenses .......................................................................................................... 45
Introduction

The Unisphere for VMAX Virtual Appliance is a VMware ESX Server virtual appliance that provides all of the components you need to manage your VMAX environment using the storsrvd daemon and Solutions Enabler network client access. These include:

- EMC Unisphere for VMAX V8.3.0.
- EMC Solutions Enabler V8.3.0 (solely intended as a SYMAPI server for Solutions Enabler client access).
- Linux OS (SUSE 11 SP3).
  Root login is not supported on SUSE 11 SP3 virtual machines.
- SMI-S Provider V8.3.0, including ECOM.

In addition, the appliances include a browser-based console to configure your storage environment. The Unisphere for VMAX vApp Manager enables you to perform configuration tasks not available in the appliances directly. Using this console, you can perform the following tasks:

- Launch Unisphere
- Monitor the application status
- Start and stop selected daemons
- Download persistent data
- Configure the nethost file (required for client access)
- Discover storage systems
- Modify options and daemon options
- Add host-based license keys
- Run a limited set of Solutions Enabler CLI commands
- Configure ESX host and gatekeeper volumes
- Load VMAX-based eLicenses
- Configure LDAP
- Configure iSCSI initiator and map iSCSI gatekeeper volumes
- Configure additional NIC card (optional)
- Download SYMAPI debug logs
- Import CA signed certificate for web browser
- Import custom certificate for storsrvd daemon
- Check disk usage
- Clear temporary files
- Restart appliance
- Configure symavoid entries
- Enable SSH
- Manage users
- Reset hostname
- Update /etc/hosts file

For information on using the Unisphere for VMAX vApp Manager, refer to its online help.
Before you begin

Before you begin to install Unisphere for VMAX Virtual Appliance, carry out the tasks in this section.

- Verify that you are installing the latest version of the appliance by checking EMC Online Support for updates.
- Verify that the client is running:
  - VMware vSphere client
  - One of the following browsers with cookies and Javascript enabled:
    - Internet Explorer 9.0 through 11.0 (Desktop only)
    - Firefox 30 or later
    - Chrome 21.0.1180 or later

  Browsers should have Flash Player 11.2 or a later release installed. If your browser has an outdated version of Flash Player, you are prompted to download the latest version when you start the web console.
- Verify that the virtual machine is not running shared memory/resources.
- Verify that the VMware ESX Server meets the following minimum requirements:

<table>
<thead>
<tr>
<th>ESX Server component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Dual-core or two CPUs</td>
</tr>
<tr>
<td>ESX Server version</td>
<td>4.0 or later</td>
</tr>
<tr>
<td>Disk space</td>
<td>120 GB</td>
</tr>
<tr>
<td>Memory</td>
<td>16GB for exclusive use by Unisphere for VMAX</td>
</tr>
</tbody>
</table>

  **Note**
  If you are upgrading to V8.3.0, the available memory is checked as part of the upgrade operation. If the requirement is not met, the upgrade is canceled.

Installing the virtual appliance directly on the ESX Server

This section describes how to install the Unisphere for VMAX Virtual Appliance directly on the ESX Server.

Step 2 has three configuration options, depending on the virtual appliance network connection:

- IPv4 only — **Step 2A: Powering on and configuring the virtual appliance (IPv4 only) on page 29.**
  Use this option if the DNS server does not support IPv6 hostnames or the DNS/ESX server is configured on an IPv4-only network.
- IPv6 only — **Step 2B: Powering on and configuring the virtual appliance (IPv6 only) on page 30.**
Use this configuration if the network configuration for the virtual appliance is IPv6 only. The virtual appliance is not able to communicate with an IPv4 host unless IPv6 packets are encapsulated inside IPv6 packets using tunneling.

- Dual stack — [Step 2C: Powering on and configuring the virtual appliance (Dual stack) on page 31.](#)

Use this configuration if the system is configured for both IPv4 and IPv6. The system supports both formats but IPv6 addresses are used for configuring the vApp Manager, SMAS and storsrvd. An IPv4 address is used only for reaching IPv4 DNS and ESX servers.

**Step 1: Installing the virtual appliance**

To install the virtual appliance:

**Procedure**

1. On the EMC Online Support site:
   
   a. Click **Support By Product** in the main navigation bar.

   b. In the Find a Product box, type **Unisphere for VMAX** and click the arrow.

   c. Locate the appropriate kit and download the OVF archive file (*.ova) containing the installation program to a temporary directory:

      *Unisphere for VMAX Virtual Appliance file name:*

      *univmaxpa820_x_suse11_x86_64_vappxxx_xxx_OVF10.ova* Where x in 820_x represents the build number. That number varies depending on when the software was built.

2. Start the vSphere Client and log in to the ESX Server on which you want to install the appliance.

3. Click **Ignore** in the security warning message.

4. From the File menu, select **Deploy OVF Template**.

5. Browse to the OVF archive file, located in the temporary directory you created earlier. Select the OVF archive file with the suffix *vappxxx_xxx_OVF10.ova*.

6. Click **Next**.

7. On the OVF Template Details page, verify the details about the appliance and click **Next**.

8. On the End User License Agreement page, select **Accept** and click **Next**.

9. On the Name and Location page, specify a name for the appliance and click **Next**.

10. On the Storage page, configure the storage options available and click **Next**.

11. On the Disk Format page, select the format in which to store the virtual machine’s virtual disks and click **Next**.

12. On the Network Mapping page, select the network you want the virtual appliance to use and click **Next**.

13. On the Ready to Complete page:

   a. Verify the information.

   b. (Optional) Select **Power on after deployment**.

   c. Click **Finish**.

14. In the Completed Successfully message, click **Close**.

---

**Installing the Unisphere for VMAX Virtual Appliance**

28  
**EMC Virtual Appliance Manager 8.3.0  Installation Guide**
Step 2A: Powering on and configuring the virtual appliance (IPv4 only)

When configuring a virtual appliance, for each prompt, type the information requested, press Enter, and then confirm that the information you entered is correct.

To power on and configure the IPv4-only virtual appliance:

Procedure
1. On the Summary page of the Virtual Infrastructure Client, click **Power On**.
2. Click the **Console** tab and watch as the appliance starts up.
3. When prompted to do so, configure an IPv4 IP address:

   Please select your static network configuration.
   For IPv4: Enter 1
   For IPv6: Enter 2
   Enter your choice [1]/2:

Select IPv4. The following information is requested:

- **IP Address [ ]**: Type the address assigned to the appliance and then type y to continue with the configuration.
  The virtual appliance uses this IP address to query the DNS server and get its hostname. Therefore, you must ensure that the IP address has a hostname mapping in the DNS server.

- **Netmask [ ]**: Type the mask of the network on which the appliance is located and then type y to continue with the configuration.

- **Gateway [ ]**: Type the gateway address to the network on which the appliance is located and then type y to continue with the configuration.

- **DNS1 [ ]**: Type the IP address of the first DNS server and then type y to continue with the configuration.

- **DNS2 [ ]**: Type the IP address of the second DNS server and then type y to continue with the configuration.

- **Is a proxy server necessary to reach the internet? y/n [n]**: Type y to configure a proxy server. For each of the following prompts, type the information requested, press Enter:
  - **ProxyServer [ ]**: Type the IP address of the proxy server and press Enter.
  - **ProxyPort [ ]**: Type the proxy port and press Enter.
Type n to continue the configuration without configuring a proxy server.

- **Do you want to set the timezone? y/[n]**:
Type **y** to set the time zone. For each of the prompts, type the information requested, press **Enter**.

- **Do you want to set host esx server? y/[n]:**
  - Type **y** to set the ESX Server. For each of the prompts, type the information requested, press **Enter**.
  - You have now finished installing the Unisphere Virtual Appliance.

4. Continue with *Step 3: Adding gatekeepers.*

**Step 2B: Powering on and configuring the virtual appliance (IPv6 only)**

When configuring a virtual appliance, for each prompt, type the information requested, press **Enter**, and then confirm that the information you entered is correct.

In an IPv6-only configuration, any DNS configured have IPv6 addresses. If you want to use one or more DNS servers with IPv4 addresses, see *Step 2C: Powering on and configuring the virtual appliance (Dual stack)* on page 31.

To power on and configure the IPv6-only virtual appliance:

**Procedure**

1. On the Summary page of the Virtual Infrastructure Client, click **Power On**.
2. Click the **Console** tab and watch as the appliance starts up.
3. When prompted to do so, configure an IPv6 IP address:

   ![Please select your static network configuration.](image)

   Select IPv6. The following information is requested:

   - **IP Address** []:
     - Type the IPv6 address assigned to the appliance.
     - The virtual appliance uses this IP address to query the DNS server and get its hostname. Therefore, you must ensure that the IP address has a hostname mapping in the DNS server.
   - **Prefix** []:
     - Type the prefix length of the network on which the appliance is located.
   - **Gateway** []:
     - Type the gateway address to the network on which the appliance is located.
   - **DNS1** []:
     - Type the IPv4/IPv6 address of the first DNS server of the network on which the appliance is located.
   - **DNS2** []:
     - Optional: Type the IPv4/IPv6 address of the second DNS server of the network on which the appliance is located.
Note

If neither of the configured DNS values are IPv4, the vApp is configured with a pure IPv6 network configuration. You cannot revert to a dual-stack network configuration at a later time.

You have now finished installing the Unisphere Virtual Appliance.


Step 2C: Powering on and configuring the virtual appliance (Dual stack)

When configuring a virtual appliance, for each prompt, type the information requested, press Enter, and then confirm that the information you entered is correct.

In a dual stack configuration, one or more of the DNS servers configured has an IPv4 address. If you want to use only DNS servers with IPv6 addresses, see Step 2B: Powering on and configuring the virtual appliance (IPv6 only) on page 30.

To power on and configure the dual stack virtual appliance:

Procedure

2. Click the Console tab and watch as the appliance starts up.
3. When prompted to do so, specify whether you want to configure an IPv4 or an IPv6 IP address:

   Please select your static network configuration.
   For IPv4: Enter 1
   For IPv6: Enter 2
   Enter your choice [1]/2:

Select IPv6. The following information is requested:

- **Does your DNS server configured supports IPv6 hostnames? y/[n]:** To continue, type y. If you type n, configuration cancels.
- **IP Address []:**
  Type the IPv6 address assigned to the appliance.
  The virtual appliance uses this IP address to query the DNS server and get its hostname. Therefore, you must ensure that the IP address has a hostname mapping in the DNS server.
- **Prefix []:**
  Type the prefix length of the network on which the appliance is located.
- **Gateway []:**
  Type the gateway address to the network on which the appliance is located.
- **DNS1 []:**
  Type the IPv6 address of the first DNS server of the network on which the appliance is located.
- **DNS2 []:**
  Optional: Type the IPv6 address of the second DNS server of the network on which the appliance is located.

You have now finished installing the Unisphere Virtual Appliance.
4. If you entered an IPv4 IP address for one or more DNS servers, you are prompted to specify additional IPv4 configuration information for those DNS servers:

- **IPv4 Address []:**
  Type the IPv4 address assigned to the appliance.
  The virtual appliance uses this IP address to query the DNS server and get its hostname. Therefore, you must ensure that the IP address has a hostname mapping in the DNS server.

- **Netmask []:**
  Type the mask of the network on which the appliance is located.

- **Gateway []:**
  Type the gateway address to the network on which the appliance is located.

- **Is a proxy server necessary to reach the internet? y/n [n]:**
  Type y to specify the IP address of the proxy server and the port.
  Type n to continue the configuration without configuring a proxy server.

- **Optional: ESX Server Name [ ]:**
  Type the fully qualified ESX Server hostname.

- **Optional: ESX Server Password [ ]:**
  Type the ESX Server password in base64 encryption format.

You have now finished installing the Unisphere Virtual Appliance.

5. Continue with *Step 3: Adding gatekeepers.*

**Step 3: Adding gatekeepers**

Solution Enabler manages VMAX arrays through gatekeeper volumes mapped to the virtual appliance as RDM pass-through volumes. The management is done through EMC proprietary commands using SCSI 3B/3C WRITE/READ commands. For every call, a WRITE command is issued to send the request, and then a READ command to get the results.

Unisphere for VMAX requires gatekeepers. For specific recommendations on the number of gatekeepers required for all VMAX configurations, refer to EMC Knowledgebase solution emc255976 available on the EMC Online Support site. To power on and configure the dual stack virtual appliance:

**Procedure**

1. Use either of the following methods to add gatekeeper volumes:

   - **Add them through the vApp Manager.** For instructions, refer to the vApp Manager online help.

     **Note**
     After adding gatekeepers through the vApp Manager, restart the SMC daemon through the vApp Manager.

     **Note**
     For ESX V4.0 and earlier, vApp Manager does not allow more than 14 gatekeeper volumes to be added to the Virtual Appliance. Attempting to add more than 14 gatekeepers returns an error message.
Present them as raw device mapping (RDM) volumes through the vSphere client. For instructions, refer to the appropriate VMware documentation.

2. Continue with Launching Unisphere or the vApp Manager on page 38.

Installing the virtual appliance through a vCenter Server

This section describes how to install the virtual appliance through a vCenter Server 4.0 and later.

Step 1: Configuring the virtual appliance

To configure the virtual appliance:

Procedure

1. On the EMC Online Support site:
   a. Click Support By Product in the main navigation bar.
   b. In the Find a Product field, type Unisphere for VMAX and click the arrow.
   c. Locate the appropriate kit and download the OVF archive file (*.ova) containing the installation program to a temporary directory: Unisphere for VMAX Virtual Appliance file name: univmaxpa820_x_suse11_x86_64_vapp_OVF10.ova

   **Note**
   In the file name above, the x in 820_x represents the build number. That number varies based on when the software was built.

2. Start the vSphere Client and log in to the vCenter Infrastructure Server through which you want to install the virtual appliance.
3. Click Ignore in the security warning message.
4. From the navigation tree, select the ESX Server on which you want to install the virtual appliance.
5. From the File menu, select Deploy OVF Template.
6. Browse to the OVF archive file, located in the temporary directory you created earlier. Select the OVF archive file with the suffix *vapp_OVF10.ova.
7. Click Next.
8. On the OVF Template Details page, verify the details about the appliance and click Next.
9. On the End User License Agreement page, select Accept and click Next.
10. On the Name and Location page, specify a name for the appliance and click Next.
11. If the resource pool is available, select it; otherwise, continue with this procedure.
12. If more than one datastore is attached to the ESX Server, select the datastore for your appliance; otherwise, continue with this procedure.
13. On the Network Mapping page, select the network you want the virtual appliance to use and click Next.
14. On the Storage page, configure the storage options presented and click Next.
15. On the Disk Format page, configure the disk format options presented and click Next.
16. On the Properties page, provide valid values for and confirm the following OVF properties:
   - IP Address
     Type the IPv4 or IPv6 address to be assigned to eth0.
   - Netmask or Prefix
     Type the netmask (IPv4 only) or prefix (IPv6 only) of the network on which the virtual appliance is located.
   - Gateway
     Type the gateway address to the network on which the appliance is located.
   - IPv4 Address for dual stack [Optional]
     IPv4 address for dual stack.
   - IPv4 Netmask for dual stack [Optional]
     IPv4 netmask address for dual stack.
   - IPv4 Gateway for dual stack [Optional]
     IPv4 gateway for address for dual stack.
   - DNS Server 1
     Type the DNS address of the network on which the appliance is located.
   - DNS Server 2
     Optional: Type the DNS address of the network on which the appliance is located.
   - Timezone
     Optional: Type the appropriate time zone.
   - Proxy Server
     Optional: Enter the IP address of the proxy server and port. For example:
     
     proxy_server_IP:port_number
   - Optional: ESX Server Name
     Enter the fully qualified ESX Server hostname.
   - Optional: ESX Server Password
     Enter the ESX Server password in base64 encryption format.

Ignore the Network Properties section that appears in vSphere V5.0 and later. Click Next.

17. On the Ready to Complete page, verify the information and click Finish.
18. In the Completed Successfully dialog, click Close.

**Step 2: Powering on the virtual appliance**

To power on the virtual appliance:

**Procedure**

2. Click the Console tab and watch as the appliance starts up.
   A Welcome screen opens. You have now finished installing the Virtual Appliance.
3. Continue with Step 3: Selecting gatekeepers on page 34.

**Step 3: Selecting gatekeepers**

Select gatekeepers as described in Step 3: Adding gatekeepers on page 32.
Installing the virtual appliance using OVFTOOL

You can install the virtual appliance through the command line from any Windows or Linux host. This section explains how to install the virtual appliance using OVFTOOL.

To install the virtual appliance using OVFTOOL, the following are required:

- vCenter Server 4.0 or a later release.
- ESX Server 4.0 or a later release managed by vCenter Server 4.x.
- VMware OVFTOOL 1.0 or a later release.

Refer to the appropriate documentation for installing vCenter Server and VMware OVFTOOL.

To install the virtual appliance using OVFTOOL:

**Procedure**

1. Install and set up the vCenter Server.
2. Add the ESX Server to the vCenter Server datacenter.
3. Install VMware OVFTOOL on a Windows or Linux host.
4. Move the Unisphere for VMAX Virtual Appliance kit to the same Linux host.
5. Run the ovftool command with necessary command line switches.

   For more information about using the command, refer to Using OVFTOOL on page 35. Unisphere for VMAX Virtual Appliance is installed and powered on automatically.
6. Add gatekeepers.
7. Continue with Launching Unisphere or the vApp Manager on page 38.

Using OVFTOOL

When deploying an IPv4-only or IPv6-only network configuration, OVFTOOL has the following syntax:

```bash
ovftool --acceptAllEulas --overwrite --powerOffTarget --powerOn
--prop:ipAddress=<IP-ADDRESS>
--prop:netmask_or_prefix=<NETMASK-OR-PREFIX>
--prop:gateway=<GATEWAY> --prop:dns1=<DNS1> --prop:dns2=<DNS2>
--prop:timezone=<TIMEZONE> --prop:esxServer=<ESX-SERVER-NAME>
--prop:encryRootPasswd=<ROOT-PASSWORD> --name=<VAPP-NAME>
--datastore=<DATASTORE> --net:Network\_1=VM\_Network
--net:Network\_2=VM\_Network --network=VM\_Network <OVA-FILE>
vii://<VCENTER ADMIN ACCOUNT>:<VCENTER-ADMIN-PASSWORD>@<VCENTER-HOST>/host/<ESX-SERVER-NAME>
```

When deploying a dual-stack network configuration, OVFTOOL has the following syntax:

```bash
ovftool --acceptAllEulas --overwrite --powerOffTarget --powerOn
--prop:ipAddress=<IP-ADDRESS>
--prop:netmask_or_prefix=<NETMASK-OR-PREFIX>
--prop:gateway=<GATEWAY> --prop:ipv4_address=<IPv4-ADDRESS>
--prop:ipv4_gateway=<IPv4-GATEWAY>
--prop:ipv4_netmask=<IPv4-NETMASK> --prop:dns1=<DNS1>
--prop:dns2=<DNS2> --prop:timezone=<TIMEZONE>
--prop:esxServer=<ESX-SERVER-NAME>
--prop:encryRootPasswd=<ROOT-PASSWORD> --name=<VAPP-NAME>
```

Installing the Unisphere for VMAX Virtual Appliance
Parameter | Description
--- | ---
IP-ADDRESS | IP address of the virtual appliance.
NETMASK-OR-PREFIX | Netmask or prefix of the virtual appliance.
GATEWAY | Gateway.
IPV4-ADDRESS | IPv4 address (Dual stack only).
IPV4-GATEWAY | IPv4 address of the gateway (Dual stack only).
IPV4-NETMASK | IPv4 netmask (Dual stack only).
DNS1 | IP address of DNS server 1.
DNS2 | IP address of DNS server 2.
TIMEZONE | Time zone setting. (Optional)
ESX-SERVER | Fully qualified hostname of ESX Server. (Optional)
ROOT-PASSWORD | Root password of ESX Server in base64 encrypted format. (Optional)
VAPP-NAME | VM Displayname
| To automatically add gatekeeper volumes during virtual appliance boot, VM Displayname must be the same as the fully qualified hostname of the virtual appliance.
DATASTORE | Name of the datastore attached to ESX Server Required only if more than one datastore is attached to ESX Server.
OVA-FILE | Absolute path of ova file.
VCENTER-HOST | Name of the vCenter.
VCENTER-ADMIN-PASSWORD | vCenter Server's Administrator password.
ESX-SERVER-NAME | ESX Server name as displayed in the vCenter Server.

Procedure
1. Install and set up the vCenter Server.
2. Add the ESX Server to the vCenter Server datacenter.
3. Install VMware OVFTOOL on a Windows or Linux host.
4. Move the Unisphere for VMAX Virtual Appliance kit to the same Linux host.
5. Run the ovftool command with necessary command line switches.
   Unisphere for VMAX Virtual Appliance is installed and powered on automatically.
6. Add gatekeepers.
7. Continue with Launching Unisphere or the vApp Manager on page 38.
Example 1 Examples

The following command is an example for an IPv4 configuration:

```bash
/usr/bin/ovftool --acceptAllEulas --overwrite --powerOffTarget --powerOn --prop:ipAddress=192.0.2.1 --prop:netmask_or_prefix=255.255.252.0 --prop:gateway=198.51.100.1 --prop:dsn1=203.0.113.1 --prop:dsn2=203.0.113.2 --prop:timezone=America/New_York --prop:esxServer=api4194.example.com --prop:encryRootPasswd=XXXXXXXXXX --name=SE_ipv4_99.example.com --datastore=api4134_local --net:Network\ 1=VM\ Network --net:Network\ 2=VM\ Network --network=VM\ Network univmaxpa820_108_suse11_x86_64_vapp_OVF10.ova vi://XXXX: XXXXXXXXXX @API4195/"vApp Build"/host/api4134.example.com
```

The following command is an example for an IPv6 configuration:

```bash
```

The following command is an example for a dual stack configuration:

```bash
/usr/bin/ovftool --acceptAllEulas --overwrite --powerOffTarget --powerOn --prop:ipAddress=2001:DB8:0:0:0:0:1:2 --prop:netmask_or_prefix=64 --prop:gateway=2001:DB8:1:0:0:0:1:2 --prop:dsn1=2001:DB8:1:0:0:0:1:2 --prop:ipv4_address=192.0.2.2 --prop:ipv4_gateway=198.51.100.2 --prop:ipv4_netmask=255.255.252.0 --prop:dsn2=2001:DB8:1:0:0:0:2:2 --prop:timezone=America/New_York --prop:esxServer=api4194.example.com --prop:encryRootPasswd= XXXXXXXX --name=SE_ipv6_1001.example.com --datastore=api4134_local --net:Network\ 1=VM\ Network --net:Network\ 2=VM\ Network --network=VM\ Network
```
Launching Unisphere or the vApp Manager

After you have installed the appliance, you can either launch Unisphere for VMAX or the vApp Manager, and/or connect to the API server through the Solutions Enabler client.

Launching Unisphere

To launch Unisphere:

Procedure

1. Type one of the following URLs in a browser:

   https://appliance_IP:unisphere_port_number  
   or

   https://appliance_host_name:unisphere_port_number

   The Unisphere port number is configured during installation. The default HTTPS port number is 8443.

   If the host IP address is an IPv6 address, surround the IP address with square brackets, for example:


   If the host IP address is an IPv4 address, type the IP address as normal, for example:

   https://198.51.100.255:8443

   For your browser to access the Unisphere for VMAX console, Flash Player 11.2 or a later release is required. Flash Player is available from the Adobe website.

2. At the login window, type the Unisphere Initial Setup User username and password, and click Login.

   The default username for the Unisphere Initial Setup User is smc and the default password is smc.

Launching the vApp Manager

To launch the vApp Manager:

Procedure

1. Type one of the following URLs in a browser:

   - https://appliance_IP:5480
   - https://appliance_host_name:5480

   If the host IP address is an IPv6 address, surround the IP address with square brackets, for example:


   If the host IP address is an IPv4 address, type the IP address as normal, for example:

   https://198.51.100.255:5480

   For either of the URLs above, the browser is redirected as shown in the following table.
2. On the log in panel, type `seconfig` for both the User and Password, and then click Login.

   The first time you login, you must change your password. The vApp Manager can also be configured to use LDAP for user authentication.

   **Note**

   When LDAP is already configured from Unisphere for VMAX, LDAP users need to be added to vApp Manager as an admin. This process requires logging into vApp Manager before disabling the local directory from Unisphere for VMAX. Unisphere for VMAX local users will not be visible in vApp Manager. For more information, refer to the vApp Manager online help.

   The vApp Manager appears. For information on using the vApp Manager, refer to its online help.

## Connecting to the API server

For instructions on connecting to the API server, refer to the *EMC Solutions Enabler Installation Guide*.

## Setting the storevntd daemon to start automatically

Ensure that the storevntd daemon is configured to start automatically.

To set the storevntd daemon to start automatically:

**Procedure**

1. On the vApp Manager dashboard, select the *Manage Daemons* tab.
2. In the Daemon column, locate the *storevntd daemon*.
3. Ensure that the button displayed in the AutoStart column has the text Unset. That is, the daemon is configured to start automatically and the only option available is to unset the auto-start property for that daemon. If necessary, set the auto-start property.

## Registering the VASA Provider with vSphere

VMware APIs for Storage Awareness (VASA) Provider improves VMware vSphere’s ability to monitor and automate storage-related operations. VASA Provider reports information about storage topology, capabilities, and status, as well as storage events and alerts to VMware. It is a standard vSphere management plug-in that is installed on each vCenter Server, and it interacts with VMware APIs for Storage Awareness.

To register the VASA Provider with vSphere:
Procedure
1. Connect to the VMware vCenter Server 5.0 or a later release using vSphere Client.
2. In the Virtual Data Center, navigate to Home > Administration > Storage Providers, and click Storage Providers in the navigator bar.
3. In the Vendor Providers pane, select Add.
4. Add the vendor provider properties (name, URL, and login information).
   For ECOM login credentials, refer to SMI-S Provider documentation.
   For the URL, use https://vapp_ip:5989/vasa/services/vasaService
   When the VASA Provider is connected, the VI Client displays the SSL certificate.
5. Click Yes to complete the registration.
6. Verify registration with vSphere:
   a. Navigate to Home > Administration > Storage Providers > Vendor Providers.
   b. Verify that the VASA Provider is listed and displays the list of managed storage systems.

Upgrading the Unisphere for VMAX Virtual Appliance using an ISO image

Periodically, EMC releases virtual appliances with security patches and hotfixes for the virtual appliance. These are available on the EMC online support website as ISO files. If you are running Unisphere for VMAX 1.6.x, or later, you can download and use an ISO upgrade file.

<table>
<thead>
<tr>
<th>From:</th>
<th>To:</th>
<th>Complete:</th>
</tr>
</thead>
</table>
| Unisphere V1.6.x or a later release | Unisphere for VMAX V8.3.0 | Step 1: Downloading the ISO upgrade file.  
Step 2: Uploading the ISO upgrade file to the datastore.  
Step 3: Mounting the ISO image.  
Step 4: Completing the upgrade. |

Before you begin

Ensure that the ESX Server minimum hardware requirements for the version to which you are upgrading are met before commencing the upgrade procedure. The available memory is checked as part of the upgrade operation and if the requirements are not met, the upgrade is canceled.

For more information about the ESX Server hardware requirements for Unisphere for VMAX Virtual Appliance, see Table 3 on page 27.

Step 1: Downloading the ISO upgrade file

Procedure
1. In a browser, navigate to the EMC Online Support site at: https://support.emc.com/
2. Locate and download the following file:
UNIVMAX820_x_se820_x_vapp_upgrade_x86_64.iso

In the file name above, x in 820_x and the x in 820_x represent software build numbers. Those numbers vary based on when the software was built.

Step 2: Uploading the ISO upgrade file to the datastore

After the download is completed, upload the ISO file to the ESC server using the VI client.

Procedure

1. Using the VI client, log in to the ESX Server.
2. In the left pane, select the ESX Server.
3. In the right pane, select the Configuration tab.
4. To list the datastores connected to the ESX Server, select Hardware > Storage.
5. Right-click the datastore and select Browse Datastore.
6. In the Datastore Browser window that displays, click Upload files. The Upload Items dialog box opens.
7. Navigate to where you saved the ISO upgrade file, select the file, and click Open.
8. In the Upload/Download Operation dialog box that displays, click Yes to accept the warning.

Step 3: Mounting the ISO image

Procedure

1. Right-click the virtual appliance and select Edit Settings.
2. On the Hardware tab, select CD/DVD Drive 1.
3. In the right pane, select Datastore ISO File and click Browse.
4. Browse to the location of the ISO file on the datastore and select the file.
5. Verify that under Device Status, the Connect at power on box is selected and click OK.

Step 4: Completing the upgrade

Procedure

1. Restart the Guest by selecting Power On Guest.
2. If the version of the vApp is V8.0.2, or lower, the upgrade cannot proceed without the required 16 GB of memory. Complete the following steps:
   a. Power off the virtual machine.
   b. Increase the memory to 16 GB.
   c. Restart the virtual machine.
3. On the Console tab, go to the virtual appliance console.
4. In the lower section of the screen, select Appliance Update from the list of options.
5. Press the Enter key to start the upgrade. After the upgrade has been completed, the console screen displays.
Re-configuring the virtual appliance IP address

You can reconfigure only the network configuration selected when the virtual appliance was first installed.

For example, if you initially set up an IPv6-only configuration, you can reconfigure the IPv6 network parameters but you cannot change it to a dual-stack configuration.

To re-configure a virtual appliance with an IPv4 address configuration:

Procedure

1. Do one of the following:
   - To re-configure a virtual appliance with an IPv4 address configuration:
     a. Log in to the vSphere client and navigate to the virtual appliance console.
     b. Use the Move Up/Move Down keys to select Configure IP and press Enter.
     c. At the following prompt, type y and press Enter to configure the static IP address:

   Do you want to configure static IP address?
   The following series of prompts enable you to reconfigure your network:

   - IP Address [ ]:
     Type a valid IP address and press the Enter key.
     The virtual appliance uses this IP address to query the DNS server and get its hostname. Therefore, you must ensure that the IP address has hostname mapping on the DNS server.

   - Netmask [ ]:
     Type the mask of the network on which the appliance is located and press the Enter key.

   - Gateway [ ]:
     Type the gateway address to the network on which the appliance is located and press the Enter key.

   - DNS1 [ ]:
     Type the first DNS server address and press the Enter key.

   - DNS2 [ ]:
     Type the second DNS server address and press the Enter key.

   - Is a proxy server necessary to reach the internet? y/[n]:
     Type y to specify the IP address of the proxy server and the port.
     Type n to continue the configuration without specifying a proxy server.

   - Are the above mentioned parameters correct? [y]/n:
     Type y to re-configure the virtual appliance IP address and return to the console.
     Type n to go back and change your responses.

   - To re-configure a virtual appliance on an IPv6-only address configured vApp:
     a. Log in to the vSphere client and navigate to the virtual appliance console.
     b. Use the Move Up/Move Down keys to select Configure IP and press Enter.
     c. The following series of prompts enable you to reconfigure your network:
Deleting the Unisphere for VMAX Virtual Appliance

To delete the Unisphere for VMAX Virtual Appliance:

Procedure

1. (Optional) If you plan to restore Unisphere and Solutions Enabler persistent data, back up the persistent data in the Unisphere for VMAX Virtual Appliance console.

2. (Optional) If you plan to restore the performance database, backup the database according to Backing up and restoring the performance database on page 44.
3. In the VMware management interface, power off the appliance.
4. Right-click on the appliance and select **Delete From Disk**.
5. Click **Yes** in the confirmation message.

**Backing up and restoring the performance database**

You can transfer performance database files between the appliance and another host for file backup and restoration. There is no facility in the appliance user interface to perform this process. However, when you are logged in to the system with the vappadmin user account, you can transfer these files.

The **vappadmin** user account is limited to performing the following commands for transferring database files:

- **passwd** — Changes the login password.
- **sftp** — Transfers database backup files into the appliance from another host, or out of the appliance to another host.
- **df** — Checks disk usage.
- **manage_spa_db_backup.sh** — Moves files between the backup location and staging location, and lists and cleans backup and staging locations.

**Backing up performance database files to another host**

From the system console, perform the following steps:

**Procedure**

1. Log in to the vApp Manager ([https://host_name:port_number](https://host_name:port_number)) and start the database backup process as described in the Unisphere help.
2. Log in to the system using the vappadmin user account. The first time that you log in, use the default password vappadmin. After you are logged in, change the password by running the passwd command, which prompts for the old and new passwords.
3. View the backup files in the backup location:
   
   ```
   manage_spa_db_backup.sh -list -backup
   ```
4. Move the backup files from the backup location to the staging location:
   
   ```
   manage_spa_db_backup.sh -stage
   ```
   This operation moves the files from the backup area to the staging area (the home directory for the vappadmin user account).
5. View the backup files in the staging location:
   
   ```
   manage_spa_db_backup.sh -list -staging
   ```
6. Transfer the backup file copies out of the appliance to the backup host. Use the following `sftp` command to access the backup host and then transfer any files ending in `.dat`.
   
   ```
   sftp user_name@fully_qualified_host_name
   ```

**Restoring performance database files from another host**

From the system console perform the following steps:
Procedure
1. Log in to the system using the vappadmin user account.
   The first time that you log in, use the default password vappadmin. After you have
   logged in, change the password by running the passwd command which prompts for
   the old and new passwords.
2. Check for available disk space: df -h.
3. Transfer the backup file copies from the backup host to the appliance. Use the
   following sftp command to access the backup host and then transfer any files ending
   in .dat.sftp user_name@fully_qualified_host_name
4. View the backup files in the staging location: manage_spa_db_backup.sh -
   list -staging
5. Move the backup files from the staging location to the backup location:
   manage_spa_db_backup.sh -restore
6. Log in to Unisphere (https://host_name:port_number) and start the database
   restore process as described in the Unisphere help.
7. After the restoration has been completed and backup files are no longer needed,
   clean the backup and staging locations: manage_spa_db_backup.sh -clean -
   all

Installing licenses

This section shows how to install VMAX-based and host-based licenses, using the virtual
appliance.

For more information on licensing, refer to the EMC Solutions Enabler Installation Guide.

Installing VMAX-based licenses

VMAX-based licenses are used to license features on VMAX arrays running Enginuity
5875 or later. These licenses are stored on the VMAX array.

Before starting this procedure, verify that the gatekeepers have been added and that the
symcfg discover command has been run from the Command Execution tab.

To install VMAX-based licenses:

Procedure
1. Open the vApp Manager.
2. Select License Validation.
3. In the eLicensing panel, click Add License File to open the Add eLicensing License
   box.
4. In the Upload License panel, click Upload License File.
5. In the file browser screen, navigate to the license file and click Open.
   A copy of the license file is transferred to the appliance.
6. In the Add Symmetrix License panel, select the VMAX array on which to install the
   license file, and click Install License.
Installing host-based licenses

Host-based licenses are used mainly to license features on VMAX arrays running Enginuity versions lower than 5875. The one exception is the TimeFinder license, which is a host-based license, regardless of Enginuity level.

To install VMAX-based licenses:

Procedure

1. Open the vApp Manager.
2. Select License Validation.
3. Type the license key (requires four characters per input box) in the SE Licensing panel and click Add.
CHAPTER 4

Installing the VASA Virtual Appliance

This chapter explains how to install the VASA Virtual Appliance in a VMware infrastructure environment. Topics include:

- Introduction .......................................................................................................... 48
- Before you begin ................................................................................................... 48
- Deploy and configure the virtual appliance .......................................................49
- Launching vApp Manager .....................................................................................50
- Adding an ESXi server ..........................................................................................50
- Adding an array ......................................................................................................51
- Mapping Fibre Channel gatekeeper devices .......................................................51
- Mounting the database LUN ..................................................................................52
- Viewing EMC VMAX VASA Provider configuration ...........................................52
- Registering EMC VMAX VASA Provider with the vSphere Web Client ...............52
- Accessing EMC VMAX VASA Provider using SSH ...........................................53
- Upgrading EMC VMAX VASA Provider ...............................................................53
Introduction

Virtual Volumes (VVols) are devices used to store application data, virtual machine configuration, swap space, and memory state. A new storage abstraction designed by VMware® with the collaboration of EMC, VVols provide storage arrays with visibility at a virtual disk level and enable them to fulfill the application's storage requirements. VVols offer more granular control to end users and increased scale beyond the previous limit of 256 logical unit numbers (LUNs) per ESXi host.

VASA (vSphere APIs for Storage Awareness) is the framework responsible for storage orchestration between VMware vSphere™ components and the VMAX system.

The VASA Provider is delivered as a virtual appliance or vApp which orchestrates the lifecycle of VVols and their derivatives: snapshots, clones, and fast-clones. It also provides storage topology, capabilities and status information to the vCenter™ and the ESXi hosts. Contained within the virtual appliance is a browser-based GUI console called vApp Manager for VASA Provider that can be used to perform VASA Provider-specific management and configuration tasks that are not handled by VMware workflows, Unisphere for VMAX or Solutions Enabler CLI.

EMC VMAX VASA Provider version 8.3.0 supports the VASA 2.0 protocol and VMAX3 and VMAX All Flash arrays running the Q3 2016 HYPERMAX OS 5977 release or later.

Before you begin

The current version of EMC VMAX VASA Provider has the following system requirements:

- The VASA Provider virtual appliance requires two virtual disks with a minimum size of 10 GB and 15 GB each.
- Configuration requires 4 GB of RAM and two Virtual Central Processing Units (vCPU).
- To host its database, EMC VMAX VASA Provider needs a Raw Device Mapping (RDM) device (for VMAX arrays only). The recommended size is 4 GB.
- A minimum of VMware vSphere 6.0 or later is required.
- Protocol Endpoints are supported only through ACLX-enabled ports.
- A redundant TCP/IP network is required.
- A minimum of five gatekeepers are required to be mapped to the virtual appliance.

**Note**

The number of gatekeepers needs to be increased in the case of multiple concurrent operations.

- A SnapVX license on the array is needed to support Snapshot operations.

**Note**

The Solutions Enabler instance embedded inside the VASA Provider vApp virtual machine is solely for EMC VMAX VASA Provider.
Deploy and configure the virtual appliance

To deploy and configure the virtual appliance:

Procedure

1. Download the OVF archive file (*.ova) containing the installation program from EMC Online Support to a temporary directory.
2. Start the vSphere Client and log in to the vCenter Infrastructure Server through which you will be installing the virtual appliance.
3. From the navigation tree, select the ESXi Server on which you will be installing the virtual appliance.
4. Right-click the ESXi Server and select **Deploy OVF Template**.
5. Browse to the OVF archive file, located in the temporary directory you created earlier. Select the OVF archive file and click **Next**.
6. On the **Review details** page, verify the details about the appliance and click **Next**.
7. On the **Accept License Agreements** page, select **Accept** and click **Next**.
8. On the **Name and Location** page, specify a name and location for the appliance and click **Next**.
9. On the **Disk Format** page, select the format in which to store the virtual machine’s virtual disks and click **Next**.
10. On the **Network Mapping** page, select the networks the deployed template should use and click **Next**.
11. On the **Customize template** page, provide valid values for the following OVF properties and then click **Next**:

   a. IP Address
   b. Netmask
   c. Gateway
   d. DNS Server 1
   e. DNS Server 2

   **Note**
   The virtual appliance uses this IP address to query the DNS Server and get its hostname. Therefore, you must ensure that the IP address has a hostname mapping in the DNS Server. The VASA Protocol will not work properly without a properly configured DNS service.

   b. Optionally, provide/select valid values for the following OVF properties:
      a. Proxy Server: Enter the IP address of the proxy server and port. For example: *ProxyServer-IP:Port*
      b. ESXi Server Name: Enter the fully qualified ESXi Server hostname.
      c. ESXi Server Password: Enter the ESXi Server password in base64 encryption format.

12. On the **Ready to Complete** page, verify the information and click **Finish**.
13. When the Completed Successfully message appears, click Close.

Launching vApp Manager

Once the vApp is deployed, follow the steps below to launch vApp Manager:

Procedure
1. Type one of the following URLs in a browser:
   
   https://appliance_IP:5480

   or

   https://appliance_host_name:5480

2. On the log in panel, type seconfig for both the User and Password, and then click Login.

   Note

   You are required to change your password from vApp Manager on first login. vApp Manager can also be configured to use LDAP for user authentication. For more information on that, refer to the vApp Manager online help.

3. vApp Manager displays. For information on using vApp Manager, refer to its online help.

Adding an ESXi server

Fibre Channel gatekeeper mapping features are unavailable until an ESXi server is attached to the appliance. The ESXi host on which the virtual machine is deployed is detected initially. To attach to a different ESXi server, the current ESXi host must be removed (see "Removing an ESXi server" section) and the new ESXi host added manually. Then select new gatekeeper devices to map (see the "Mapping Fibre Channel gatekeeper devices" section).

Procedure
1. Log into the vApp Manager and select Map Gatekeepers > Fibre Channel.

   This view shows the unmapped and mapped Fibre Channel gatekeeper devices. If there is no ESXi server attached to the appliance, no devices display. All gatekeeper configuration features are unavailable until an ESXi server is added.

2. Click Add ESXi, and type the following:
   
   - Server name (fully qualified server name)
   - ESXi server user name
   - ESXi server password
   - Re-enter ESXi server password
3. Click Add.

Results
The ESXi server name displays next to Host ESXi Attached.

Adding an array

Add an array that the VASA Provider will be managing to the ESXi server to create devices available for mapping.

Procedure
1. Log into the vApp Manager and select Map Gatekeepers > Fibre Channel.
2. Next to the Host ESXi name, click Add Array.
3. The Select Array dialog opens. Select the checkbox next to the desired array ID and then click Add Array.
   The Devices attached to the Host ESXi list shows the devices that are available for mapping to the Virtual Appliance machine.

Mapping Fibre Channel gatekeeper devices

Before you begin
If no ESXi server is attached to the appliance, then mapping features are unavailable. See Adding an ESXi server on page 50.
Fibre Channel gatekeeper devices are mapped to the appliance through the ESXi server attached to the appliance. If no ESXi server is attached to the appliance, this tab allows for adding a server.

Procedure
1. Log into the vApp Manager and select Map Gatekeepers > Add Array > Select Array.
   This view shows the unmapped and mapped Fibre Channel gatekeeper devices.
2. Click Refresh to update the list of mapped and unmapped devices.
3. In the Devices attached to the Host ESXi [Available for mapping to the Virtual Appliance machine] list, click the checkbox next to the device(s) you want to map and then click Map Devices.

Note
If you toggle away from the Map Gatekeepers tab to another tab in the management screen, you will be required to re-add the array before seeing and mapping devices.
Mounting the database LUN

EMC VMAX VASA Provider requires that a separate TDEV device is mapped to host the database. The recommended size is 4 GB.

Procedure
1. Log into the vApp Manager and select Map Gatekeepers > Add Array > Select Array.
2. In the Devices attached to the Host ESX list, under the Map Device column, click Map next to the device that will be used as the database LUN.
   The device is moved from the Devices attached to the Host ESX list to the Devices attached to Virtual Appliance Host list.
3. In the Devices attached to Virtual Appliance Host list, under the Mount DB column, click MountDB next to the device.
   An information dialog confirms that the device has been successfully mounted.

Viewing EMC VMAX VASA Provider configuration

Procedure
1. Log into vApp Manager and select the Command Execution tab.
2. Select the VP Configuration panel to see the settings and their default values:
   - VP log file size (MB)—Default is 64 megabytes.
   - VP log level—Default is INFO.
   - Number of log files to be retained—Default is 10.
   - Max concurrent connections per session—Default is 4.
   - Retain VP certificate—Default is false.

   **Note**
   For self-signed certificates on multiple vCenters this setting needs to be set to True.

   - SYMAPi debug log—Default is disabled.

Registering EMC VMAX VASA Provider with the vSphere Web Client

The default EMC VMAX VASA Provider credentials for registration are "admin" for user name and "#1Password" for password. In the interests of security EMC recommends changing the default values. The default registration credentials can be changed at https://[applicance_IP]:5989/ecomconfig > "Change Password".

**Note**
EMC recommends that users don’t change other options within the ECOMConfig portal.
Procedure
1. From the Navigator panel of the VMware vSphere Web Client for vCenter, select the vCenter in the Hosts and Clusters view.
2. Under the Manage tab, select Storage Providers and click on the + symbol.
   The New Storage Provider dialog opens.
3. Fill out the name, user name, password and URL and click OK.

   **Note**
   The VASA Provider URL is https://vAppHostName:5989/vasa-providers.xml

4. Click Yes to the Security Alert dialog that asks if you want to trust the host.
5. To verify the registration, refresh the view in the vSphere Web Client. The EMC VMAX VASA Provider and its details should be listed.

   **Note**
   Users need to rescan from vCenter to discover the newly created storage containers.

### Accessing EMC VMAX VASA Provider using SSH

#### Before you begin
The default user name and password for logging into EMC VMAX VASA Provider through SSH is "cseadmin".

#### Procedure
1. Log into the vApp Manager and select the Command Execution tab.
2. Select Host Configuration> Enable SSH.

### Upgrading EMC VMAX VASA Provider

#### Note
This procedure applies when upgrading the EMC VMAX VASA Provider from the previous release to the current release.

#### Procedure
1. Take a snapshot of the vApp before beginning the upgrade. This can be used to restore the vApp if the upgrade procedure fails.
2. Upload the ISO image into the ESXi Server Datastore on which EMC VMAX VASA Provider is deployed.
3. Start the vSphere Client and log into the vCenter Infrastructure Server through which you will be upgrading the virtual appliance.
4. On the lefthand menu click on Data Store and select the ESXi Datastore.
5. Click on Manage from the top menu and navigate to the files.
6. Click on the upload icon on the righthand side to upload the ISO update file.
7. To mount the ISO image on the virtual appliance's CD drive, right-click the virtual appliance and select Edit Settings.
8. On the **Virtual Hardware** tab, select CD/DVD Drive 1.

9. From the drop-down menu, select **Datastore ISO File** and click **Browse** to locate the ISO image in the data store.

10. Click **OK** to exit the dialog box.

11. Go to the **Console** tab of the virtual appliance and using the Move Up/Down keys select **Appliance Update**.

12. Press Enter to perform the update.

   The update will take a few minutes, after which the virtual appliance will reboot and the screen will show the main console of the latest version.

---

**Note**

You can use the welcome screens of the virtual appliance and vApp Manager to confirm that EMC VMAX VASA Provider has been updated correctly.
INDEX

V
Virtual Appliance
  installing through a vCenter Server 20
  installing using OVFTOOL 21

deleting 24
installing directly to the ESX Server 17
overview 16
prerequisites 17