Active System Manager Release 8.3
User's Guide

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

© **2016 Dell Inc. or its subsidiaries. All rights reserved.** This product is protected by U.S. and international copyright and intellectual property laws. Dell and the Dell logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

2016 - 09

Rev. A01

Contents

1

Overview

Active System Manager (ASM) is Dell's unified management product that provides a comprehensive infrastructure and workload automation solution for IT administrators and teams. ASM simplifies and automates the management of heterogeneous environments enabling IT to respond more rapidly to dynamic business needs.

IT organizations today are often burdened by complex data centers that contain a mix of technologies from different vendors and cumbersome operational tasks for delivering services while managing the underlying infrastructure. These tasks are typically performed through multiple management consoles for different physical and virtual resources, which can dramatically slow down service deployment.

ASM features a user interface that provides an intuitive, end-to-end infrastructure and workload automation experience through a unified console. This speeds up workload delivery and streamlines infrastructure management, enabling IT organizations to accelerate service delivery and time to value for customers.

What can you do with ASM?

ASM provides capabilities and benefits that allow organizations to:

- **Accelerate IT service delivery** by automating and centralizing key operational functions like workload and infrastructure deployment.
- **Free up IT staff** to focus on higher priority projects by dramatically reducing manual steps and human touch points.
- **Use infrastructure more fully and efficiently** by pooling available server, storage and network resources that you can schedule for future use or allocate on demand.
- **Standardize workload delivery** processes to ensure accuracy and consistency for initial deployment, while maintaining the flexibility to scale workloads according to business needs.
- **Maximize investments in both Dell and Non-Dell IT resources** with support for heterogeneous IT environments.

How is ASM different?

ASM helps you realize these benefits through a unique set of features and capabilities designed for IT administrators. These capabilities include:

- **Template-based provisioning and orchestration** — Simplify IT service delivery with a centralized approach for capturing and applying workload-specific configuration and best practices; plus step-by-step definition and execution of tasks across the workload lifecycle.
- **Infrastructure lifecycle management** — Easily manage the entire infrastructure lifecycle with:
  - Fast discovery, inventory, and initial configuration of assets.
  - Full lifecycle management of physical and virtual infrastructure and workloads.
- **Deep virtualization integration** — Manage cluster-level and virtual machine (VM) lifecycle.
- **Resource pooling and dynamic allocation** — Optimize capital expenditures by creating and managing physical and virtual IT resource pools.
- **Radically simplified management** — Powerful and intuitive user interface that makes it easy to set up, deploy, and manage your IT environment and enables simplified integration with third-party tools.

- **Open and extensible** — An architecture that integrates with the IT of today and tomorrow; this means being able to plug a new solution into your existing architecture, as well as giving you flexibility in the future to adopt new technical innovations.

ASM makes it easy to automate IT service delivery and to manage your IT environment end-to-end. You can improve and accelerate service and infrastructure delivery, maximize efficiency across your IT service lifecycle, and consistently achieve high-quality IT services.

About this document

This document version is updated for ASM release 8.3.

What's New in this Release

Active System Manager 8.3 is focused on expanding capabilities around workload deployment, adding new capabilities around managing existing environments, and improving the granularity of information shown around the current state of environments under management.

The highlights of Active System Manager release 8.3 include the following:

Support for Dell Hybrid Cloud for Virtualization that includes a new plug-in for compatibility with vRealize Orchestrator 7.0 and 7.1. Customers can create workflow that automates the deployment of ASM service templates created in ASM.

This release also includes compatibility support for the following:

- Support for SUSE Linux Enterprise Server 11 SP4 that enables Dell's SAP HANA Cloud Solution to leverage ASM's hardware compatibility list to offer ASM automation capabilities to customers.
- Support for PowerEdge R630, PowerEdge R730, PowerEdge R730XD hybrid and flash configurations, PowerEdge FC430, PowerEdge FC630, and PowerEdge FX2- All flash configurations. Customers can leverage ASM capabilities to discover, deploy and manage the VSAN ready nodes on Virtual SAN 6.2.

Accessing Online Help

Active System Manager (ASM) online help system provides context-sensitive help available from every page in the ASM user interface.

Log in to ASM user interface with the user name **admin** and then enter password **admin**, and press Enter.

After you log in to ASM user interface, you can access the online help in any of the following ways:

- To open context-sensitive online help for the active page, click? , and then click **Help**.
- To open context-sensitive online help for a dialog box, click**?** in the dialog box.

Also, in the online help, use the **Enter search items** option in the **Table of Contents** to search for a specific topic or keyword.

Other documents you may need

In addition to this guide, the following documents available on the Dell Support website at **dell.com/support/manuals** provide additional information about ASM.

Go to **dell.com/asmdocs** for more supporting documents such as:

- *Active System Manager Release 8.3 Release Notes*
- *Active System Manager Release 8.3 Installation Guide*

- *Active System Manager Release 8.3 Compatibility Matrix Guide*
- *Active System Manager Release 8.3 API Reference Guide*
- *Active System Manager Release 8.2 SDK Reference Guide*
- *Active System Manager Integration for VMware vRealize Orchestrator User's Guide*

For more information about ASM, including how-to videos, white papers, and blogs, see the Active System Manager page on Dell TechCenter:

http://www.dell.com/asmtechcenter

Contacting Dell Technical Support

To contact Dell Technical Support, make sure that the Active System Manager Service Tag is available.

- Go to the tech direct portal https://techdirect.dell.com
- Login using your existing account or create an account if you do not have an account.
- Create a case for your incident.
- Add your Active system Manager Service Tag
- Select **Active System Manager** as the Incident type.
- Type relevant information in the Problem Details, and add attachments or screenshots if necessary.
- Fill in contact information and submit the request.

Licensing

ASM licensing is based on the total number of managed resources, except for the VMware vCenter and Windows SCVMM instances.

ASM 8.3 supports following license types:

- Trial License — A trial license can be procured through the account team and it supports up to 25 resources for 90 days.
- Standard License — A standard license grants full access.

You receive an email from customer service with instructions for downloading ASM and your license.

If you are using ASM for the first time, you must upload the license file using the **Initial Setup** wizard. To upload and activate subsequent licenses, click **Settings → Virtual Appliance Management.**

1. Under the **License Management** section, on the **Virtual Appliance Management** page, click **Add**. The **License Management** window is displayed.
2. Click **Browse** beside **Upload License** and select an evaluation license file, and then click **Open**.

   The **License Management** window with the license type, number of resources, and expiration date of the uploaded license is displayed.
3. Click **Save** to apply the evaluation license.
4. After uploading the license file, the following information about the license is displayed:
   - License Type
   - Number of Resources
   - Number of Used Resources
   - Number of Available Resources
5. To replace the evaluation license with standard license, click **Add** under **License Management** section, click **Browse** beside **Upload License** and select a regular standard license file, and then click **Open**.

   You get information regarding license type, number of resources and expiration date of the uploaded license on License Management window.

6. Click **Save** to apply the standard license.
   It replaces the evaluation license with standard license.

After uploading the license file, the following information about the license is displayed:

- License Type
- Number of Resources
- Number of Used Resources
- Number of Available Resources

You can add multiple standard licenses. After uploading multiple licenses, all the licenses are aggregated together and displayed as one under **License Management** section.

NOTE: If you try to upload the same standard license second time, you get an error message stating that License has already been used.

2

Getting started with ASM 8.3

When you log in to ASM for the first time, the **Getting Started** page is displayed. This page provides a recommended guided workflow for getting started with ASM. A check mark on each step indicates that you have completed the step.

NOTE: After logging in to ASM for the first time, you can initially set up the configurations.

NOTE: The Getting Started page is not displayed for standard users.

NOTE: Ensure that you log in using `admin` as the user name and `password`.

The steps include:

- **Step 1: Define Networks** — Click **Define Networks** to define networks that are currently configured in your environment for resources to access. You can also click **Settings** → **Network** to define, edit, or delete the existing network. For more information about defining networks, see Define Networks.
- **Step 2: Discover Resources** — Click **Discover Resources** to discover one or more resources (Chassis, Server, Switch, Storage, SCVMM, vCenter, and Element Manager) that you want ASM to manage on your network. Also, following information is displayed on the **Discover** pane. For more information about discovering resources, see Discovering Resources.
  - **Discovered Resources** — Indicates the number of resources that are discovered in ASM.
  - **Pending Resources** — Indicates that discovery is in progress for the number of resources displayed.
  - **Errors** — Indicates that ASM is unable to discover the number of resources displayed due to some issues.
- **Step 3: Define Existing Service** — Click **Define Existing Service** to discover and import existing VMware clusters in the environment and add it as a service in ASM.
- **Step 4: Configure Resources** — Click **Configure Resources** to perform a firmware compliance check on the discovered resources and configure the chassis as needed.
- **Step 5: Publish Templates** — Click **Publish Templates** to open the **Templates** page. On the **Templates** page, create a template or clone a sample template, edit the cloned template, and publish it. The templates ready to be deployed after they are published.

If you do not want to view the **Getting Started** page when you log in next time, clear the **Show welcome screen on next launch** check box at the bottom of the page. However, to revisit the **Getting Started** page, from the **Active System Manager** drop-down menu, select **Getting Started** or from the **Settings** drop-down menu, select **Getting Started**.

Related links

Discovery overview
Initial Setup
Discovering resources
Templates
Defining or editing existing network
Configuring resources or chassis

3

Initial Setup

The Initial Setup wizard enables you to configure the basic settings required to start using ASM.

Before you begin, ensure that you have the following information available:

- The local network share that contains the ASM license.
- The time zone of the virtual appliance that hosts ASM.
- The IP address or host name of at least one Network Time Protocol (NTP) server.
- The IP address or host name, port, and credentials of the proxy server. (Optional)
- The networks in your environment for ASM to access. (Optional)

To configure the basic settings:

1. On the **Welcome** page, read the instructions and click **Next**.
2. On the **Licensing** page, select a valid license, type the ASM Service Tag, and click **Save and Continue**.
3. On the **Time Zone and NTP Settings** page, configure the time zone of the virtual appliance, add the NTP server information, and then click **Save and Continue**.
4. (Optional) On the **Proxy Settings** page, select the **Use a proxy server** check box, enter the configuration details, and then click **Save and Continue**.
5. (Optional) If you want to configure ASM appliance as a DHCP or PXE server, on the **DHCP Settings** page, select the **Enable DHCP/PXE server** check box, enter the DHCP details, and then click **Save and Continue**.
6. On the **Summary** page, verify the license, time zone, proxy server, and DHCP settings.
7. Click **Finish** to complete the initial setup.

After the initial setup is complete, if you want to edit the NTP, proxy server, DHCP settings, and license information, click **Settings** in the left pane, and then click **Virtual Appliance Management**.

Related links

Uploading license
Configuring time zone and NTP settings
Configuring proxy settings
Configure DHCP settings

Uploading license

If you are using ASM for the first time, you must upload the license file using the **Initial Setup** wizard. To upload a subsequent license, click **Settings** in the left pane, and then click **Virtual Appliance Management**. On the **Virtual Appliance Management** page, click **Edit** in the **License Management** section.

1. On the **Licensing** page of the Initial Setup wizard, click **Browse**, and select a valid license file.
   The following information is displayed based on the license selected:
   - **Type** — Displays the license type. There are two valid license types supported in ASM:
     - Standard — Full-access license type.

- Trial — Evaluation license that expires after 90 days and supports up to 25 resources.
- **Total Resources** — Displays the maximum number of resources allowed by the license.
- **Expiration Date** — Displays the expiry date of the license.

2. To activate the license, click **Save and Continue**.

Related links

License management

Configuring time zone and NTP settings

On the **Time Zone and NTP Settings** page of the **Initial Setup** wizard, you can set the time zone of the virtual appliance that hosts ASM and configure the Network Time Protocol (NTP) servers used for time synchronization.

NOTE: Configuring NTP adjusts your ASM system time. Your current user session ends if the time is adjusted forward. The time will sync 5–10 minutes after this step. If this occurs, log in to ASM again and continue with the setup process.

NOTE: When adding NTP server settings in the OS section of a server component, if more than one NTP server is necessary, ensure to separate the IP addresses using a comma (,).

1. On the **Time Zone and NTP Settings** page of the **Initial Setup** wizard, from the **Time Zone** drop-down list, select the time zone in which the virtual appliance operates.
2. To synchronize the time with the NTP server, enter the IP address or Fully Qualified Domain Name (FQDN) of a **Preferred NTP Server** and **Secondary NTP Server** (optional).
3. Click **Save and Continue**.

After the initial setup is complete, to change NTP server information, click **Setting** → **Virtual Appliance Management**. On the **Virtual Appliance Management** page, click **Edit** in the **Time Zone and NTP Settings** section.

Related links

Editing default time zone and NTP settings

Configuring proxy settings

If your environment uses a proxy server to communicate with external services, then you must configure the proxy server settings in ASM.

To enable communication using a proxy server:

1. On the **Proxy Settings** page of the **Initial Setup** wizard, select the **Use a proxy server** check box.
2. In the **Server IP Address** box, enter the IP address or host name for the proxy server.
3. In the **Port** box, enter the port number for the proxy server.
4. If the proxy server requires credentials to log in, select the **Use Proxy Credentials** check box, enter the **User Name** and **Password**, and then reenter the password to confirm.
5. To test the connection to the proxy server, click **Test Proxy Connection**.
6. Click **Save and Continue**.

After the initial setup is complete, click **Settings** → **Virtual Appliance Management** to change the proxy settings. On the **Virtual Appliance Management** page, click **Edit** in the **Proxy Settings** section.

Related links

Editing proxy settings

Configure DHCP settings

Configure the following settings to set the ASM appliance as a DHCP or PXE server.

NOTE: If you want to configure the DHCP server on a particular VLAN that has one or more DHCP servers already configured, then make sure to turn off the other DHCP servers on the VLAN.

1. On the **DHCP Settings** page, select the **Enable DHCP/PXE Server** check box.

   NOTE: The Enable DHCP/PXE Server check box is not selected by default.
2. In the **Subnet** box, enter the IP address of the subnet on which DHCP server can be operated.
3. In the **Netmask** box, enter the subnet mask that is used by DHCP clients.
4. In the **DHCP Scope Starting IP Address** box, enter the starting IP address in the range assigned to the clients.
5. In the **DHCP Scope Ending IP Address** box, enter the ending IP address in the range assigned to the clients.
6. In the **Default Lease Time (DD:hh: mm: ss)** box, enter the default time that an IP address is granted to a client.

   NOTE: It is recommended to set the default lease time for a short duration, ranging from one to three hours.
7. In the **Max Leave Time (DD:hh: mm: ss)** box, enter the amount of time that an IP address is granted to a client.
8. In the **Default Gateway** box, enter the gateway address. This address is used by the DHCP clients as the default gateway.
9. In the **DNS Server** box, enter the domain name system (DNS) domain name of this DHCP scope to use with one or more DNS servers.
10. Click **Save** and **Continue**.

    It may take 15 to 20 seconds to enable the DHCP server.

Verifying initial setup

1. On the **Summary** page, verify the settings you have configured in the previous pages.
2. If the information is correct, click **Finish** to complete the initial setup.
3. If you want to edit any of the information, click **Back** or click the corresponding page name in the left pane.

4

Dashboard

The **Dashboard** displays the following information:

NOTE: For standard users, only the details of the services they have created or for which they have permission is displayed.

- The **Service Overview** section displays a graphical representation of the services based on the state, total number of services deployed, and state icons that represent the service state. The number next to each icon indicates how many services are in a particular state. The services are categorized based on the following states:
  - **Critical** (red band on the graphic): Indicates the services for which the deployment process is incomplete due to errors.
  - **Healthy** (green band on the graphic): Indicates that the service is successfully deployed and is healthy.
  - **In Progress** (blue band on the graphic): Indicates the services for which deployment is in progress.
  - **Warning** (yellow band on the graphic): Indicates that the resources in a service are in a state that requires corrective action, but does not affect the overall system health. For example, the firmware version installed on a resource in the service is not compliant.

    You can even monitor the health of the server in a service by viewing the status of the service on the **Service** page.

    NOTE: If the service is in Yellow or Warning state, it indicates that one or more servers or storage is in a failed state. If the service is in Red or Error state, it indicates that the service has fewer than two servers or storage that are not in a failed state. If the service has only one server or one storage, the service health reflects the server or storage's health.

    To view the status of the failed server component, hover the cursor on the image of the failed component in the service.

    To display a list of services in a particular state, click the corresponding color bands on the graphic: red, blue, green, or yellow. The following information about the services is listed below the graphical display:

    * State icons.
    * Service name — Click to view detailed information about the service.
    * Name of the user who deployed the service.
    * Date and time when the service was deployed.
    * The number of resources used by the particular service based on the component type.
    * Errors, if any.

    From the **Service History** drop-down list, you can select one of the following options to filter and view the service deployments.

    * **All Deployments**
    * **Last 10 Deployments**
    * **Last Week**
    * **Last Month**
    * **Last 6 Months**
    * **Last Year**
- **Resource Overview** — Indicates the numbers of chassis, servers, switches, and storage that have been discovered.

Under **Server Health**, the image indicates the following:

- **Healthy** (green band on the graphic): Indicates that there is no issue with the servers and that servers are working as expected.
- **Critical** (red band on the graphic): Indicates that critical problems exist with one or more components in the server. These issues must be fixed immediately.
- **Warning** (yellow band on the graphic): Indicates that the servers are in a state that require corrective action, but does not affect overall system health. For example, the firmware running on a server is not at the required level or not compliant.
- **Unknown** (gray band on the graphic): Indicates that the state of the server is unknown.

- Under **Server Utilization in Services**, a pie chart displays:
  - **Servers In Use** (blue band on the pie chart) — Indicates exact number of servers that are in use. To view the total number of servers used, move the pointer over the band.
  - **Servers Available** (gray band on the graphic) — Indicates the exact number of servers that are available for deployment. To view the number of servers that are available, move the pointer over the band.
- Under **Utilization by Server Pool**, each bar represents a server pool and displays the number of servers used and available in that server pool.
- Under **Total Storage Capacity**, a pie chart displays the percentage of storage disk space currently being used.
  - **Storage Used** (blue band on the graphic) — Indicates the percentage of used storage disk space. To view the percentage of used storage disk space, move the pointer over the band.
  - **Storage Available** (gray band on the graphic) — Indicates the percentage of available disk storage space. To view the percentage of available storage space, move the pointer over the band.
- Under **Capacity by Storage Group**, each bar represents one of the following storage groups and displays the storage capacity used or available on the particular storage group.
  - **Dell EqualLogic Group**
  - **Dell Compellent Arrays**
  - **NetApp Arrays**

The **Dashboard** also displays the following information in the right pane:

- **Licensing Information** — Displayed when any one of the following events occur:
  - The number of resources managed by ASM exceeds the valid license count.
  - The trial license expires.
- **Quick Action** — Enables you to create a template, add existing service, and deploy a new service.
- **Recent Activity —** Lists the most recent user and system initiated activities. Click **View All** to view the activities on the **Logs** page.

  Also, the following information is displayed on the **Dashboard**.
  - **Discovered Resources** — Indicates the number of resources that are discovered in ASM.
  - **Pending Resources** — Indicates that the discovery is in progress for the number of resources displayed.
  - **Errors** — Indicates that ASM is unable discover the number of resources displayed due to some errors.
- Links to learn more about service deployments and templates.

Related links

Viewing service details
Service states
Deploying service

Service states

Table 1. Service states

State	Icon	Description
Critical		Indicates service deployed is failed due to some issues.
Warning		Indicates that one of the resources that are part of a service is in a state that requires corrective action, however this does not affect the overall health of the system. For example, the firmware running on the resource is not at the required level or not compliant.
In Progress		Indicates that the deployment of the service is in progress.
Healthy		Indicates that the service is successfully deployed and is healthy.

Related links

Dashboard

5

Services

A service is a deployment of a published template.

NOTE: For standard users, only the details of the services they have created or for which they have permission is displayed.

The **Services** page displays the services that are in the following states in both Graphical and Tabular view.

- **Critical** — Displays the number of services for which the deployment process is incomplete due to errors.
- **Healthy** — Indicates that the service is successfully deployed and is healthy.
- **In Progress** — Indicates that services for which deployment is in progress.
- **Warning** — Indicates that one or more resources in a service require corrective action.

On the **Services** page, you can:

- Click **Deploy New Service** to deploy a new service. For more information on deploying a new service, see Deploying service.

  NOTE: Standard users are allowed to deploy services that they have created or for which they have permissions.
- Click **Add Existing Service** to add an existing service. For more information on adding an existing service, see Adding an existing service.
- Click **Export All** to export all the service details to .csv file.

To switch between Graphical and Tabular view, click the Graphic icon or Tabular icon next to the **View As** option.

To view the services based on a particular service state, select one of the following options from the **Filter By** drop-down list. Alternately, in the Graphical view, click the graphic in a particular state.

- **All**
- **Critical**
- **Healthy**
- **In progress**
- **Warning**

In the Graphical view, each square title represents a service and has the status of the service at the bottom of the graphic. The state icon on the graphic indicates the state of the service. The components in blue indicate the component types that are included in the deployment. The components that are in gray indicate the component types that are not included in the service.

In the Tabular view, the following information is displayed:

- **Status** — Indicates the status of the service.
- **Name** — Indicates the name of the service.
- **Deployed By** — Indicates the name of the user who deployed the service.
- **Deployed On** — Indicates the date and time when the service is deployed.

Click the service in the Tabular or Graphical view to view the following information about the service in the right pane:

- Service name and description to identify the service.

- Name of the user who deployed the service.
- Date and time when the service is deployed.
- Displays the name of the reference template used in the service.
- Lists the number of resources included in the service for deployment, based on the following component types:
  - Application
  - Virtual Machine
  - Cluster
  - Server
  - Storage
- Click **View Details** to view more details about the service.
- Click **Update Firmware** to update the firmware of one or more servers in the service that are not compliant.
- Click **Export to File** to export the specific service details to **.csv** file.

Related links

Viewing service details
Deploying service

Deploying service

NOTE: You cannot deploy a service using a template that is in draft state. Publish the template before you use the template to deploy a service.

To deploy a service:

1. Click **Active System Manager** → **Services**.

   The **Services** page is displayed.
2. On the **Services** page, click **Deploy New Service**.

   The **Deploy Service** wizard is displayed.
3. On the **Deploy Service** page, perform the following steps, and then click **Next**.
   a. From the **Select Published Template** drop-down list, select the template to deploy a service.
   b. Enter the **Service Name** (required) and **Service Description** (optional) that identifies the service.
   c. Type a number that indicates the number of deployments that is required for a service.
   d. If you want to update the firmware and software version running on the servers that are in the service, select the **Manage Server Firmware** check box, and from the **Use Firmware Repository** drop-down, select a firmware repository.

      NOTE: Changing the firmware repository may update the firmware level on servers for this service. Firmware on shared devices will still be maintained by the global default firmware repository.
   e. If you want to grant permission for Standard users to use this service, under **Manage Service Permissions**, select the **In addition to all Admins, grant Standard Users access to this service** check box, and perform one of the following actions:
      - To grant access to all Standard users, select the **All Standard Users** check box.
      - To grant access only to specific Standard users, select the **Specific Standard Users** check box, and perform the following tasks:
        a. Click **Add User(s)** to add one or more Standard users to the list.

           To remove a Standard user from the list, select the Standard user and click **Remove User(s)**.

b. After adding the Standard users, select or clear the check box next to the Standard users to grant or block access to the service.

4. On the **Deployment Settings** page, configure the required settings, and click **Next**.

   a. To manually enter the IP address, click **User Entered IP**.
   b. From the **IP Source** drop-down menu, select **Manual Entry**.
   c. Type IP address in the **Static IP Address** text box.

   NOTE: You can manually enter the IP Address only for Static network.

   NOTE: Select the Retry On Failure option to ensure that ASM selects another server from the server pool for deployment if any server fails.

   NOTE: Each server may be retried up to five times.

5. Click **View All Settings** to view the details of the components that are part of the service.
6. On the **Schedule Deployment** page, perform one of the following tasks:

   - **Deploy Now** — Select this option to deploy the service immediately.
   - **Schedule Later** — Select this option to enter the date and time to deploy the service later.

NOTE:
You must manually configure network and BIOS on Dell PowerEdge C6220 servers.

Before configuring ensure that:

- There is sufficient hard disk space available on the server to install the operating system.
- Single NIC is set to PXE boot.
- Single NIC is set as a first boot device and the hard disk is set as second boot device.
- The network is set as workload network for Windows and Linux bare-metal operating system installation and is set as hypervisor management network for ESXi deployment.

You must configure the network on the top of rack switch that is connected to the PowerEdge C6220 server and also configure any VLAN on the server facing port of the top of rack switch. To configure the VLAN, ensure that the PXE VLAN is untagged for any operating system deployment.

NOTE: Prior to deployment of FX2 or Blade server, you need to disable Flexaddress every server in chassis. To disable Flexaddress, follow the path:
CMC > **Server Overview** > **Setup** > **FlexAddress.**

You need to make sure that server is powered down to disable FlexAddress. Ideally these should be done prior discovering the server.

Add existing service

With ASM 8.3, you can discover and import existing VMware clusters in the environment and add it as a service in ASM. After adding the existing service, you can manage the resources in the cluster by updating the firmware of the components in the cluster or deleting the components in the cluster.

CAUTION: Deleting a component from the service also deletes the component from the data center environment.

NOTE: Before adding an existing service, you must ensure that the components such as servers, vCenter, or storage that are part of the cluster are discovered by ASM in the Resource list and are in Reserved or Available state.

Adding an existing service

To add an existing service:

1. Click **Service**.
2. Click **+ Add Existing Service**.
3. On the **Add Existing Service** page, type a service name in the **Name** field.
4. Select the **Firmware Compliance** check box to perform firmware updates on the components in the cluster.
5. Click **Next**.
6. On the **Cluster Component** page, under the **Basic Settings** section, type a name for the cluster component in the **Component Name** field.
7. Under the **Cluster Settings** section, select the following:
   a. **Target Virtual Machine Manager** — Select the vCenter name where the cluster is available.
   b. **Data Center Name** — Select the data center name where the cluster is available.
   c. **Cluster Name** — Select the cluster name you want to discover.
8. Click **Next**.
   The list of all the resources available in the cluster are displayed on the **Summary** page.

   NOTE: If the resources are discovered and in available or reserved state the Available Inventory displays the components as Yes.
9. Click **Finish**.

After the service is created, you can update firmware, change firmware baseline, and delete resources in a service.

CAUTION: Deleting resources from existing services deletes the component from the service and the environment.

Viewing service details

The **Service Details** page displays the state of the service at component level in Topology and Tabular view.

- In the Topology view, under **Service Resources**, you can view the topology of the components and connections as structured in a selected service template.

  In the Topology view, the color of the component icons indicates the following:

  – The red component icon indicates that the service is not deployed on a particular component due to some issues.
  – The blue component icon indicates that the service is successfully deployed on the components.
  – The light blue component icon indicates that the service deployment is in progress.
  – The yellow icon indicates that particular component requires firmware update.

  To view the following information about the resources, click the corresponding component icons.

  – IP Address (Click the IP address of a Dell resource to open the Element Manager.)
  – Hypervisor IP Address (for servers only)
  – Deployment state
  – OS IP address
- In the Tabular view, under **Service Resources**, the following information is displayed based on the resource types in the service.

  – Under **Virtual Machines**, you can view the following information about the virtual machines configured on the clusters:

    * **Hostname**
    * **OS Type**

    - **CPUs**
    - **Disk Size**
    - **Memory**
  - Under **Clusters**, you can view the following information about the clusters created on VMware vCenter or Microsoft virtualization environments:
    - **IP Address**
    - **Asset/Service Tag**
  - Under **Physical Servers**, you can view the following information about the servers that are part of a service:
    - **Hostname**
    - **IP Address**
    - **Hypervisor IP Address**
    - **Asset/Service Tag**
  - Under **Storage**, you can view the following information and view the volumes created on a particular storage and the size of the volumes.
    - **IP Address**
    - **Asset/Service Tag**
- Under **Service Information**, you can view the following information:
  - Name of the service
  - **Overall Service Health** — Displays health of the service. The overall service health is determined by the following:
    - **Resource Health** — Displays the health monitoring of resources reported by Dell OpenManage Plug-in for Nagios Core.
    - **Firmware Compliance** — Displays if the resources are firmware-compliant. This option is applicable only if you have enabled firmware update on the service.
    - **Deployment State** — Indicates if the deployment of the service completed successfully.

Table 2. Service States

Service State	Icon	Description
In Progress		Indicates that service deployment is in progress.
Critical		Indicates that service deployment is failed due to some issues.
Healthy		Indicates that service is deployed successfully and the resources are firmware complaint and healthy.
Warning		Indicates that the one of more resources that are part of a service is in a state that requires corrective action, but does not affect overall system health. For example, the firmware running on the resource is not at the required level or not compliant.

View Logs — To view logs, select the component icon of a deployed service from the **Component States** window on **Service Information** page, you get **View Logs** link. Click the **View Logs** link, you get **In progress**, **Error**, **Successful**, **Warning**, **Informational** log from View Logs. This is varied with deployed service.

  - **Deployed By** — Displays the name of the user who deployed the service.
  - **Deployed On** — Displays the date and time when the service is deployed.
  - **Reference Template** — Displays the name of the reference template used in the service.

NOTE: For existing services the name is displayed as User Generated Template and not a template name from the inventory.

- **Reference Firmware Repository** — Displays the reference firmware repository.
- **User Permissions** — Displays one of the following:
  - **Enabled** — Indicates that the permission is granted for one or more Standard users to deploy this service.
  - **Disabled** — Indicates that the permission is not granted for Standard users to deploy this service.

Under **Service Actions**:

- Click **Delete** to delete a service or resources in the service.

  NOTE: Deleting resources from existing services, deletes the component from the service and the data center environment.
- Click **Retry** to redeploy a failed service.
- Click **View All Settings** to view the settings configured on the resources in a service for deployment.
- Click **Export to File** to export the service details to a .csv file.
- Click **Generate troubleshooting bundle** link, you can generate a compressed file of ASM logs files which are used for trouble shooting.

Under **Resource Actions**:

- From the **Add Resources** drop-down list, select the type of the resources that you want to add to the service.
  From this drop-down menu, you can even select **Network** to update workload network.

  For more information regarding **Add Network**, see Add Network.
- If you need to input data for the template which is used to create the running service, then the **Upgrade Components** button is displayed. Click the **Upgrade Components** buttons, **Update Service Component** window is displayed. Fields in the **Update Service Component** window vary depending on templates. Fill in all the displayed fields it. Click **Save**.
- Click **Migrate Server(s)** to migrate a server's settings to another server in a designated server pool. Alternatively, to migrate a server's settings, click the server component icon on the topology view, and click **Migrate Server(s)**.

  NOTE: The migrate server is only available for Boot from SAN deployments.
- Click **Delete Resources** to delete resources from a service.

Under **Firmware Actions**:

To update the firmware on out of compliant servers within the service, click the **Update Server Firmware** button.

To change the firmware baseline on a server, click **Change Server Firmware Baseline**.

Under **Recent Activity**:

The component deployment status and information on the current deployed service is displayed.

Related links

Deploying service
Exporting service details
Updating firmware
Retrying service
Adding components to an existing service deployment
Deleting service
Deleting resources from service
Migrating servers
Upgrading components

Viewing the compliance report

The following are the steps to view the firmware and software compliance report.

1. On the home page, click **Services**.
2. Select a service to view the compliance report.
3. In the right pane, click **View Details**.
   The **Service Details** page is displayed.
4. On the **Service Details** page, click **View Compliance Report**.
   The **Server Firmware/Software Compliance Report** page is displayed.
   You can also view the compliance status on the **Server Firmware/Software Compliance Report** page.
5. Click **Firmware Components** to view the firmware components.
6. Click **Software Components** to view the software components.

NOTE: To update the noncompliant resources, click Update Resources.

Component deployment states

After you deploy a service, ASM assigns one or more states to the components based on the deployment status.

The following are different types of states displayed at a component level:

- Pending — Indicates that, within a service, the deployment is not yet started for the particular components.
- In Progress — Indicates that, within a service, service deployment is in progress for the particular components.
- Complete — Indicates that, within a service, the service deployment is completed for the particular components.
- Critical — Indicates that, with in a service, service deployment is not successful for the particular components.
- Cancel — Indicates that, within a failed service, deployment is not yet started for the particular components and canceled due to other component (s) deployment failure.

Editing service information

To edit the information of a service:

1. On the home page, click **Services**.
2. On the **Services** page, click the service, and in the right pane of the services detail page, click **View Details**.
3. On the **Service Details** page, in the right pane beside click **Edit**.
4. In the **Edit Service Information** dialog box, perform the following steps:

   a. Modify the **Service Name** and **Service Description** that identifies the service.

   b. If you want to update the firmware and software running on the servers that are part of the service, select the **Manage Server Firmware** check box, and from the **Use Firmware Repository** drop-down list, select a firmware repository.

   NOTE: Changing the firmware repository may update the firmware level on servers for this service. Firmware on shared devices will still be maintained by the global default firmware repository.

   c. If you want to grant permission for Standard users to use this service, under **Manage Service Permissions**, select the **In addition to all Admins, grant Standard Users access to this service** check box, and perform one of the following actions:

   - To grant access to all Standard users for this service, select **All Standard Users** option.
   - To grant access only to specific Standard users for this service, select **Specific Standard Users** option, and perform the following tasks:

a. Click **Add User(s)** to add one or more Standard users to the list.

   To remove the Standard user from the list, select the Standard user and click **Remove User(s)**.

b. After adding the Standard users, select or clear the check box next to the Standard users to grant or block access to the service.

c. Click **Save**.

Deleting service

To delete a service, perform the following steps:

NOTE: Standard users are allowed only to delete the service that they have deployed.

NOTE: Deleting a service deletes the VLANs configured on the switches.

1. On the home page, click **Services**.
2. On the **Services** page, click the service, and in the right pane of the services detail page, click **View Details**.
3. On the **Service Details** page, in the right pane, under **Service Actions**, click **Delete**.
4. In the **Delete Service** dialog box, perform the following steps:

   NOTE: Deleting a shared resource could affect other running services.

   a. The **Return Servers to resource Pool** check box is selected by default. This process returns the IP/IQNs assigned to the servers that were a part of the service and returns the servers to the server pool. After the service is deleted, the Dell servers that were part of the deleted service are rebooted, and the servers are set to PXE boot ready for the next deployment. The servers that are selected by default for tear down are turned off after the service is torn down.

   b. The **Delete VMs** check box is selected by default to delete the VMs created on the cluster. The servers and VMs are selected by default for tear down.

   c. Select the **Delete Cluster(s) and Remove from Hyper-V and vCenter** check box to remove the clusters created on Hyper-V or vCenter and removes the Hyper-V and vCenter instances. Servers and VMs are selected by default for tear down.

   d. Select the **Delete Storage Volume(s)** check box to remove the storage volumes created during the service deployment.

Exporting service details

This feature enables you to export the service details to a .csv file.

1. On the **Services** page, click **Export to File** in the right pane.
2. Open and save the .csv file.

Retrying service

You can redeploy a service for which deployment is not successful due to some issues.

NOTE: Standard users can only redeploy a failed service that they have deployed.

1. On the home page, click **Services**.
   The **Services** page is displayed.
2. Select a service in an error state and click **View Details** in the right pane.
   The **Service Details** page is displayed.
3. In the right pane, under **Service Actions**, click **Retry**.
   Click **Yes** when a confirmation message appears.

Viewing all settings

The **View All Settings** page displays all the component settings used to configure the resources in the deployment of the service.

- For more details about the Application properties, see Application Settings.
- For more details about the Virtual Machine properties, see Virtual Machine Settings.
- For more details about the Cluster properties, see Cluster Settings.
- For more details about the Server properties, see Server Settings.
- For more details about the Storage properties, see Storage Settings.

Migrating servers (service mobility)

In ASM, service mobility refers to the capability to migrate server's BIOS, NICs, storage connectivity, and assigned identity information to another server in a designated server pool, to perform planned maintenance or service activities or to respond to a hardware fault or failure issue.

Currently, migration is supported only for boot form SAN server, and it is supported only for bare metal OS installs of Linux or Windows. It is not supported for ESXi. Therefore, the migration will not affect the virtual machines.

It is recommended only to migrate between identically configured hardware. Different operating systems may not boot correctly on hardware that is different.

Migration pre-requisites

- ASM does not install operating systems on the boot from SAN volume. Therefore, you must install operating system on the servers prior to migration.
- Make sure that the free servers are available in the server pool for migration, and it is compatible.
- During the migration, the operating systems will not be booted. Therefore, it is recommended to shut down the server before migrating the boot from SAN image.
- It is recommended to configure a server pool that has servers with same model, RAID, and networking devices, including the specific slot to which network resources are connected.

Related links

Migrating servers

Migrating servers

NOTE: Standard users can migrate the servers that are part of the server pool for with they have permission.

You can migrate only one server at a time. However, after a successful migration, extra servers can be migrated. During migration, ASM tries to identify an exact match for the hardware. If it is not available in the server pool, a different hardware can be selected.

You may encounter some issues during configuration of the new servers. In such scenarios, you can address the issues preventing the proper configuration of the target server, and retry the deployment.

To migrate a server's configuration to a different server pool:

1. On the **Service Details** page, perform one of the following actions:
   - In the topology view, click a server component, and click **Migrate** in the box that is displayed
   - In the topology view, click a server component, and click **Migrate** in the right page.
2. In the **Migrate Server(s)** dialog box, in the **State** column, select the server, and then in the **New Server Pool** column, select the designated server pool to migrate.

NOTE: When you boot from SAN, you always get a migrate option on Service Details page. Migrate is not available for any other type of deployment so in that case, you do not get Migrate Server option Service Details page.

Upgrading components

If an upgrade to ASM has added new required fields to components within the template from which the service was deployed, the Upgrade Components button is displayed. While this action is not mandatory, certain service or resource functions are not available until this upgrade has been completed.

Click on the **Upgrade Components** button to launch the **Update Service Component** window. Fields in this window vary depending on which components contain newly required settings. Complete all the displayed fields. Click **Save**.

Adding components to an existing service deployment

After a successful service deployment, you can add one or more application, storage, server, cluster, and virtual machine components to an existing service.

NOTE: Standard users are allowed only to add components to a service for which they have permission.

NOTE: You can add components even if they are currently not in the template. For example, if you have storage, server and cluster, you can still add VM.

NOTE: You can add components to a service for which deployment is successful or to a failed service deployment.

To add components to a service:

1. On the home page, click **Services**.
   The **Services** page is displayed.
2. Select a service and click **View Details** in the right pane.
   The **Server Details** page is displayed.
3. In the right pane, under **Resource Actions**, from the **Add Resources** drop-down menu, click one of the following components:
   - **Application** — Enables you to add one or more applications to the service.
   - **VM** — Enables you to add one or more virtual machines to the service.
   - **Cluster** — Enables you to add one or more clusters to the service.
   - **Server** — Enables you to add one or more servers to the service.
   - **Storage** — Enables you to add one or more storage components to the service.
   - **Network** — Enables you to add one or more networks to the service.

Related links

Adding storage to existing service
Adding servers to existing service
Adding virtual machines to existing service
Adding application

Adding virtual machines to existing service

To add virtual machines to an existing service:

1. On the **Add VM(s)** page, add a virtual machine by one of the following ways:
   - If you want to clone a virtual machine configuration, next to **New Component Settings**, click **Duplicate**, and perform the following steps:
     1. From the **Resource to Duplicate** drop-down list, select a virtual machine to clone.

2. In the **# of Instances** box, enter the number of new virtual machines that you want to add to the service. Click **Continue**.
3. In the **Component Name** box, enter the virtual machine name for one or more virtual machines.
4. In the **Host Name** box, enter the host name of the virtual machines.

- If you want to add new virtual machine, click **New**, and perform the following steps:

1. From the **Select a Component** drop-down list, select one of the following:
   - **vCenter Virtual Machine**
   - **Clone vCenter Virtual Machine**
   - **Clone Hyper-V Virtual Machine**
2. Under **Associated Resources**, select the existing components to associate with the newly added virtual machine.
3. Click **Continue**.

   Based on the component type, specific settings and properties appear automatically that are required and can be edited. For more information specific to component type settings, see Component Types.

2. Click **Save**.

Adding servers to existing service

To add a server to an existing service:

On the **Add Server(s)** page, add the servers to the service in one of the following ways:

- If you want to clone an existing server configuration to the servers that you want to add to the service, next to **New Component Settings**, click **Duplicate**, and perform the following steps:

1. From the **Resource to Duplicate** drop-down list, select a server.
2. In the **# of Instances** box, enter the number of server instances that you want to add to the service. Click **Continue**.
3. In the **Component Name** box, enter the name of the corresponding servers.
4. In the **Server Pool** box, enter the name of the server pool.
5. In the **Host Name** box, enter the host name for the corresponding servers.
6. Click **Save**.

- If you want to add new server component, next to **New Component Settings**, click **New**, and perform the following steps:

1. From the **Select a Component** drop-down list, select a server component.
2. Under **Associated Resources**, perform one of the following actions:
   - When you are adding a new component to a template, if you want to associate the component with all the existing components, select **Associate All resources** option.

     The new component automatically associated with the existing components.
   - When you are adding a new component to a template, if you want to associate the component only with the selected components, select **Associate Selected Resources**, and then select the components to associate as needed.

   Based on the component type, specific settings and properties appear automatically that are required and can be edited. For more information specific to component type settings, see Component Types.

When you redeploy an existing service after adding one or more servers, the following states are displayed in the **Resources** page:

- The state of the existing server resources that are part of the service changes from “Deployed” to ‘Deploying”, and then changes to “Deployed” after the deployment is complete.

- The state of the new server changes from “Not In Use” to “Pending”. Once the deployment starts, the state changes to “Deploying”. If the deployment is successful, the state changes to “Deployed”. If the deployment is not successful, the state changes to “Critical”.

Adding storage to existing service

To add storage components to an existing service:

1. On the **Add Storage** page, add the storage to the service by following the steps mentioned here:
   - If you want to add new storage component, perform the following steps:
     1. From the **Select a Component** drop-down list, select one of the following storage components:
        - **Compellent**
        - **EqualLogic**
        - **NetApp**
        - **VNX**
     2. Under **Associated Resources**, to associate the newly added storage component to the existing components in the service, select the components to associate.
     3. Click **Continue**.

        Based on the component type, specific settings and properties appear automatically that are required and can be edited. For more information-specific component type settings, see Component Types.
2. Click **Save**.

Adding Network

You can update workload network using **Add Network** feature.

1. On the home page, click **Services**.
2. Select a service for which you want to add a network, in the right pane, click **View Details**.
3. Under **Resource Action**, from the **Add Resources** drop-down list, select **Network**.
   The **Add Network** window is displayed.
   All the used resources and networks are displayed under **Resource Name** and **Networks**.
4. From the **Available Networks** drop-down menu, select the network, and click **Add**.
   The selected network is displayed under **Network Name**.
   Also, you can define a new network by clicking **Define a new network**.
5. Select **Port Group** from the **Select Port Group** drop-down menu.
6. Select resources from the **Select Resources** drop-down menu.
7. Click **Save**.

NOTE: To remove the added network, under Actions, click Remove.

Adding application to an existing service

To add application to an existing service:

1. On the home page, click **Services**.
2. Select the service you want to add application and click **View Details** on the right pane.
   The service details page is displayed.
3. In the right pane, from the **Add Resources** drop-down menu, select **Applications**.
   For more information on adding application, seeAdding application.

NOTE: To stop managing an application, on the Service Details page, click application icon on the resource, and then click Stop Managing Applications. If you click Stop Managing Applications, the application icon on the resource is no longer available. But the application remains on the VM or server.

Deleting resources from service

1. On the **Delete Resources from Service** page, select the resources that you want delete from the service.
2. Click **Delete**.

NOTE: Deleting a shared resource may affect other running services.

6

Templates

A Template is a collection of components. It defines the end state of your infrastructure that is configured when a service is generated.

A Template may consist of various components that identify the type of resource to be configured. In ASM, each component is categorized as:

- Application
- Virtual Machine
- Cluster
- Server
- Storage

The Templates page allows you to access default Dell templates or create templates that can be used to deploy services. For example, you can create a template for deploying a physical server, deploy VMs in new or existing ESXi clusters and so on.

NOTE: Standard users are allowed only to view and use the templates for which administrator has granted the permissions.

After creating a Template, you can then publish a template for deployment.

NOTE: It is recommended to first provision the physical devices, then deploy virtual components, and lastly configure applications.

After creating a template, a template is automatically saved in a Draft state and not yet published. A template must be published to be deployed.

NOTE: A template in Draft state cannot be deployed.

Template States

- **Draft:** A template created but not yet published.
- **Published:** A template ready for deployment.

On **Template** page, You get two options:

- **My Templates**
- **Sample Templates**

Under **My templates**, two tasks can be performed:

- **Create Template**
- **Upload External Template**
- **Export All**

If you select **Sample Template**, you get templates which are integrated with ASM by default.

Related links

Managing templates
About roles
Cloning template
Deleting template
Creating template
Editing template
Building and publishing template
Importing template

Managing templates

The **Templates** page displays the information about the templates in Graphical and Tabular format. To switch between the Graphical and Tabular view, click the Graph icon or Table icon next to **View As** option on the top of the **Templates** page. To sort and view the templates based on categories, in the **Filter By** drop-down list, select a category. Alternatively, in the Graphical format click the graphic that represents a category to view the templates under a category.

NOTE: Standard users are allowed only to view the details of the template for which administrator has granted the permissions.

The Graphical view displays the following:

- Displays the Draft and Published templates. Each graphic in this view indicates a template. A template with a label DRAFT indicates it is a draft template.
- In a Template graphic, the component icons in blue indicate that the particular components are part of the template. The component icons in gray indicate that the particular components are not part of the template.

The Tabular view displays the following information about the template

- **State** — Indicates the state of the template: Draft or Published
- **Category** — Indicates the template category.
- **Name** — Indicates the name of the template.
- **Last Deployed On** — Indicates the date and time when the templates is used for deployment.

You can click on a specific template to see the following details of the template in the right pane:

- Template name and description for the template.
- **Category** — Indicates the template category.
- **Created on** — Indicates the date and time of template creation.
- **Created by** — Indicates the name of the user who created the template.
- **Updated on** — Indicates the date and time when the template was last updated.
- **Updated by** — Indicates the name of the person who last updated the template
- **Last Deployed on** — Indicates date and time when the selected template was last deployed.

From this page, you can:

NOTE: Only the user with Administrator role has the permissions to create, edit, delete, publish, import, and clone templates.

- Click **Create Template** on the top of the **Templates** page to create a template.
- Click the template and perform the following actions in the right pane:
  - Click **Edit** to edit the template.

- Click **Delete** to delete the Template
- Click **Deploy Service** to use the specific template for service deployment.
- Click **View Details** to view the resources that can be configured using the template and connections.
- Click **Clone** to use the properties of this template and create a template.

Related links

Creating template
Editing template
Deleting template
Cloning template
Importing template
Deploying service

Viewing template details

To view more details about a template:

1. On the **Templates** page, select a template.
2. In the right pane, click **View Details**.
   The topology of the components that are part of the template is displayed in the Template Builder.
3. To view all the component settings, on the **Template Builder** page, click **View All Settings** in the right pane.
   The **Template Settings** dialog box lists the details about the component configured in the template. For more information about the components settings, see Component Types.

Related links

Component types

Creating template

The **Create Template** feature allows you to either create a template or clone the components of an existing template into a new template.

To create a template or clone an existing template, perform the following steps:

1. In the left pane, click **Templates**.
2. On the **Templates** page, click **Create Template**.
   The **Create Template** dialog box is displayed.
3. Select either **New** or **Clone Existing** option.
   If there is **Clone Existing**, select any existing template that is to be cloned. The components of the selected template are cloned into the new template.
4. Enter a **Template Name**.
5. From the **Template Category** drop-down list, select a template category. To create a category, select **Create New Category** from the list.
6. Enter **Template Description**. (Optional).
7. If you want to update the firmware and software running on the servers when you deploy a service that uses this template, select the **Manage Server Firmware** check box, and from the **Use Firmware Repository** drop-down menu, select a firmware repository.

   NOTE: Changing the firmware repository may update the firmware level on servers for this service. Firmware on shared devices will still be maintained by the global default firmware repository.
8. If you want to grant permission to Standard users to use this template, under **Manage Service Permissions**, select the **In addition to all Admins, grant Standard Users access to this service** check box, and perform one of the following actions:
   - To grant access to all Standard users to this template, select **All Standard Users** option.

- To grant access only to specific Standard users to use this template, select **Specific Standard Users** option, and perform the following tasks:
  1. Click **Add User(s)** to add one more Standard user to list displayed.

     To remove the Standard user from the list, select the Standard user and click **Remove User(s)**.
  2. After adding the Standard users, select or clear the check box next to the Standard users to grant or block access to use this template.

9. Click **Save**.

Related links

Building template overview
Building and publishing template
Editing template information
Importing template
Exporting template
Deleting template
Cloning template

Editing template information

To edit the template information:

1. In the left pane, click **Templates**.
2. On the **Templates** page, click the template that you want to edit, and click **Edit** in the right pane.

   The **Template Builder** page is displayed.
3. In the right pane, click **Edit**.
4. In the **Template Name** box, modify the template name as needed.
5. From the **Template Category** drop-down list, select a template category. To create a category, select **Create New Category** from the list.
6. In the **Template Description** box, enter the description for the template.
7. If you want to update the firmware and software running on the servers when you deploy a service that uses this template, select **Manage Server Firmware** check box, and from the **Use Firmware Repository** drop-down menu, select a firmware repository.

   NOTE: Changing the firmware repository may update the firmware level on servers for this service. Firmware on shared devices will still be maintained by the global default firmware repository.
8. If you want to grant permission to Standard users to use this template, under **Manage Service Permissions**, select the **In addition to all Admins, grant Standard Users access to this template** check box, and perform one of the following actions:
   - To grant access to all Standard users to this template, click **All Standard Users**.
   - To grant access only to specific Standard users to use this template, click **Specific Standard Users**, and perform the following tasks:
     1. To add one more Standard user to the list, click **Add User(s)**.

        To remove a Standard user from the list, select the Standard user and click **Remove User(s)**.
     2. After adding or removing the Standard users, select or clear the check box next to the Standard users to grant or block access to use this template.
9. Click **Save**.

Building template overview

The **Template Builder** page allows you to build a customized template by configuring both physical and virtual components. On the **Template Builder** page, you can set the component properties. For example, you can create a template that just provisions physical servers with OS on them, or creates storage volumes, creates clusters or VMs, or deploy applications on VMs.

This page displays the graphical representation of the topology created within a particular template.

NOTE: Initially, a newly created or a cloned template appears in a Draft state on the Template page and remains in the same state until published.

The following component types can be configured in a template:

- Storage
- Server
- Cluster
- Virtual Machine
- Application

NOTE: While building a template, it is recommended to first provision the physical resources, then configure virtual resources and lastly configure application settings to be deployed on the resources.

On this page, you can:

- Build and Publish a template
- Delete a Template
- Import a Template
- Deploy a Service

NOTE: The Deploy Service functionality is applicable only on published templates.

Related links

Building and publishing template

Building and publishing template

After creating a template using the **Create Template** dialog box, to start building a customized template using the Template Builder page, perform the following steps:

1. To add a component type to your template, click the respective component icon on top of the Template Builder.
   The corresponding **<component type> component** dialog box is displayed.
2. From the **Select a Component** drop-down list, select the component that you want to add.
3. In the **# of Instances** box, enter the number of component instances that you want to include in a template.
4. Under **Associated Resources**, perform one of the following actions:
   - When you are adding a new component to a template, if you want to associate the component with all the existing components, click **Associate All resources**.

     The new component automatically associated with the existing components.
   - When you are adding a new component to a template, if you want to associate the component only with the selected components, click **Associate Selected Resources**, and then select the components to associate as needed.

   Based on the component type, specific settings and properties appear automatically that are required and can be edited. For more information about the specific component type settings, see Component Types.
5. Click **Add** to add the component to the **Template Builder**.
6. Repeat the steps 1 through 5 to add multiple components.
7. After you complete adding components to your template, click **Publish Template**. Publishing a template indicates that a template is ready for deployment.
   If a template is not published, it cannot be deployed and remains in the Draft state until published.
8. After publishing a template, you can use the template to deploy a service in the **Services** page.

Related links

Building template overview

Deploying service

Importing template

The **Import Template** option allows you to import the components of an existing template, along with their component configurations, into a template. For example, you can create a template that defines specific cluster and virtual machine topology, and then import this template definition into another template. After importing, you can modify the component properties of the imported components.

NOTE: Editing the imported template does not affect the original template that was imported and vice versa.

To import a template, perform the following steps:

1. Click **Templates**.
2. On the **Templates** page, select the template which you want to import, in the right pane, click **Edit** to edit an existing template.
3. On the Template Builder page, in the right pane, click **Import Template**.
4. In the **Import Template** dialog box, select a specific template from the **Select a template** drop-down list, and click **Import**.

Exporting template

To export template, perform the following tasks:

1. On the home page, click **Templates**.
2. Select the template which you want to export.
3. In the right pane, click **Export Template**.
4. **Export Template to ZIP File** window is displayed. The window contains:
   - **File Name**
   - **Use Encryption Password from Backup Setting**

   File Name:

   Enter template name in **File Name** field.

   Use Encryption Password from Backup Setting:

   Select **Use Encryption Password from Backup Setting** if you have set encryption password in Backup setting. Deselect **Use Encryption Password from Backup Setting** if you have not set encryption password in Backup setting.
5. After you deselect the option two more fields are displayed:
   - **Set File Encryption Password**
   - **Confirm Encryption Password**

   Set File Encryption Password:

   Enter encryption password in **Set File Encryption Password**.

   Confirm Encryption Password:

   To confirm encryption password, confirm that encryption password reenter encryption password in Confirm Encryption Password.
6. Click **Export to File**. After clicking **Export to File**, the file gets downloaded in download directory. A window is displayed to save the exported file. There **save file** option is selected by default.
7. Click **Ok** to save the file.

Uploading external template

To upload a template which has imported from other instances of ASM:

1. On the home page, click **Templates**.
2. Click **Upload External Template** to upload the exported template.

   The **Upload External Template** page is displayed.

   For more information on exporting template, see Exporting Template.
3. Click **Browse** to select the exported file from your directory.
4. Select the **Use Encryption Password from Backup Settings** check box, if you have set the encryption password in Backup and Restore.

   Clear the **Use Encryption Password from Backup Settings** check box if you have not set the encryption password in Backup and Restore.

   If you clear the **Use Encryption Password from Backup Settings**, you must enter the encryption password in the **Encryption Password** field.
5. Type the template name in the **Template Name** field.
6. Select a template category from the **Template Category** drop-down menu.

   Select the **Create New Category** option if you want to create a template category.
7. In the **Template Description** box, type description for the template.
8. To update the firmware and software while deploying a service using this template, select the **Manage Server Firmware/ Software** check box and select a firmware and software repository from the **Use Firmware/Software Repository** drop-down menu.

   NOTE: Changing the firmware repository may update the firmware level on servers for this service. Firmware on shared devices is maintained by the global default firmware repository.
9. To grant access to standard users to use this template, select the **Manage Service Permissions** check box, click any one of the following options:
   - **All Standard Users** — Select this option to provide access to all standard users.
   - **Specific Standard Users** — Select this option to provide access to specific users. Click **+ Add User(s)** to add the users. To remove users added to list, select the user and click **Remove User(s)**.
10. Click **Upload and Continue**.

    The **Additional Settings** page is displayed.
11. Under **Network Settings**, select new network from the **Select New Network** drop-down menu.
12. Under **OS Settings**, do the following:
    a. Type the OS administrator password in the **OS Administrator Password** box.
    b. Select the new OS repository from the Select **New OS Repository** drop-down menu.
13. Under **Server Pool Settings**, select the new server pool from the **Select New Server Pool** drop-down menu.
14. Click **Finish**.

Editing template

You can edit an existing template to change the draft state of the selected template to the published state for deployment, or to modify the exiting components and their properties.

To edit a template, perform the following steps:

1. Click **Templates**.
2. Select a template, and click **Edit**.
3. Perform the necessary changes to the template.
4. Click **Publish Template** to make the template ready for deployment

From this page, you can:

- To edit the template information, click **Edit** next to the Template Information section title.
- View the following information about the template in the Template Information section:
  - **Category** — Displays the template category.
  - **Reference Firmware Repository** — Displays the reference firmware repository.
  - **User Permissions** — Displays one of the following:
    - **Disabled** — Indicates the permission to access the template is not granted to any Standard users.
    - **Enabled** — Indicates that the permission is granted to one or more Standard users.
  - Under **Actions**, you can:
    - To publish the template, click **Publish Template**. Once it is published, it can be deployed as a service.
    - To delete the template, click **Delete Template**.
    - To view all the resources that are in the template and their properties, click **View All Settings**.
    - To import the configuration from an existing template, click **Import Template**.

Viewing template details

To view more details about a template:

1. On the **Templates** page, select a template.
2. In the right pane, click **View Details**.
   The topology of the components that are part of the template is displayed in the Template Builder.
3. To view all the component settings, on the **Template Builder** page, click **View All Settings** in the right pane.
   The **Template Settings** dialog box lists the details about the component configured in the template. For more information about the components settings, see Component Types.

Related links

Component types

Deleting template

The **Delete** option allows you to delete a template from ASM.

To delete a template:

1. Click **Templates** and select the template to be deleted, and click **Delete**. You can also delete a selected template from the **Template Builder** page.
2. Click **YES** when a warning message is displayed.

Cloning template

The **Clone** option allows you to copy an existing template into a new template. A cloned template contains the components that existed in the original template. You can edit it to add more components or modify the cloned components. To clone an existing template, perform the following steps:

1. On the home page, click **Template**.
2. Select a template, in the right pane, click **Clone**.
   The **Cone Template** page is displayed.
3. Type a template name in the **Template Name** box.
4. Select a template category from the **Template Category** drop-down menu.
   Select the **Create New Category** option if you want to create a template category.
5. In the **Template Description** box, type description for the template.
6. To update the firmware and software while deploying a service using this template, select the **Manage Server Firmware/ Software** check box and select a firmware and software repository from the **Use Firmware/Software Repository** drop-down menu.

NOTE: Changing the firmware repository may update the firmware level on servers for this service. Firmware on shared devices is maintained by the global default firmware repository.

7. To grant access to standard users to use this template, click the **Manage Service Permissions** check box, select any one of the following options:
   - **All Standard Users** — Select this option to provide access to all standard users.
   - **Specific Standard Users** — Select this option to provide access to specific users. Click **+ Add User(s)** to add the users. To remove users added to list, select the user and click **Remove User(s)**.
8. Click **Next**.

   The **Additional Settings** page is displayed.
9. Under **Network Settings**, select new network from the **Select New Network** drop-down menu.
10. Under **OS Settings**, do the following:
    a. Type the OS administrator password in the **OS Administrator Password** box.
    b. Select the new OS repository from the **Select New OS Repository** drop-down menu.
11. Under **Server Pool Settings**, select the new server pool from the **Select New Server Pool** drop-down menu.
12. Click **Finish**.

Deploying service

NOTE: You cannot deploy a service using a template that is in draft state. Publish the template before you use the template to deploy a service.

To deploy a service:

1. On the home page, click **Services**.

   The **Services** page is displayed.
2. On the **Services** page, click **Deploy New Service**.

   The **Deploy Service** wizard is displayed.
3. On the **Service Information** page, perform the following steps, and click **Next**.
   a. From the **Select Published Template** drop-down list, select the template to deploy a service.
   b. Enter the **Service Name** (required) and **Service Description** (optional) that identifies the service.
   c. If you want to update the firmware and software running on the servers that are part of the service, select **Manage Server Firmware** check box, and from the **Use Firmware Repository** drop-down, select a firmware repository.

      NOTE: Changing the firmware repository may update the firmware level on servers for this service. Firmware on shared devices will still be maintained by the global default firmware repository.
   d. Type a number that indicates the number of deployments that is required for a service.
   e. If you want to grant permission for Standard users to use this service, under **Manage Service Permissions**, select the **In addition to all Admins, grant Standard Users access to this service** check box, and perform one of the following actions:
      - To grant access to all Standard users for this service, select **All Standard Users** option.
      - To grant access only to specific Standard users for this service, select **Specific Standard Users** option, and perform the following tasks:
        a. To add one or more Standard users to the list, click **Add User(s)**.

           To remove the Standard user from the list, select the Standard user and click **Remove User(s)**.
        b. After adding the Standard users, select or clear the check box next to the Standard users to grant or block access to the service.
4. Click **Next**.

   The **Deployment Settings** wizard is displayed.
5. On the **Deployment Settings** page, configure the required settings and click **Next**.

   Configuring Hardware Settings:

a. Select server source from the **Server Source** drop-down menu.

   You can select **Server Pool** or **Manual Entry** from **Server Source** drop-down menu.

b. Select server pool from the **Server Pool** drop-down menu.

   If you select **Server Pool** from the **Server Source** drop-down menu, in that case you can view all user-defined server pools along with the Global pool. Standard users can see only the pools that they have permission.

   If you select **Manual Entry**, instead of **Server Pool**, **Choose Server** drop-down menu is displayed. From the **Choose Server** drop-down menu, you can manually select server with its service tag for deployment from the list under the **Choose Server** drop-down menu.

   NOTE: Select the Retry On Failure option to ensure that ASM selects another server from the server pool for deployment if any server fails.

   NOTE: Each server may be retried up to five times.

   Configuring OS Settings:

c. Under **OS Settings** section, from IP Source, click **ASM Selected IP** or **User Entered IP**.

   1. To manually enter the IP address, click **User Entered IP**.
   2. From the **IP Source** drop-down menu, select **Manual Entry**.
   3. Type IP address in the **Static IP Address** text box.

6. In the **Schedule Deployment** page, perform one of the following actions:
   - **Deploy Now** — Select this option to deploy the service immediately.
   - **Schedule Later** — Select this option and enter the date and time to deploy the service.

Related links

Adding components to an existing service deployment
Retrying service
Deleting service

Deploying multiple instances of service

NOTE: You cannot deploy a service using a template that is in draft state. Publish the template before you use the template to deploy a service.

To deploy multiple instances of service, you must perform the following tasks:

1. On the **Template** page, select a template.
2. Click **Deploy Service**. **Deploy Service** window is displayed.
3. On the **Deploy Service** window, under **Service Information**:
   - Select template from the **Select Published Template** drop-down menu.
   - Enter service name in **Service Name** field.

   NOTE: For the multiple instances of deployment, this service name is the base name for the service which needs to be deployed. The first service is called by the name which is provided in Service Name field. Rest of the services are indicated by number after base service name.
4. Type the number of deployments in **Number of Deployments** fields.
5. Click **Next**. It directs you to **Deployment Settings** in the **Deploy Service** window.

   NOTE: When deploying multiple instances of a service, Autogeneration of hostname is required to be configured in a template. When this option is enabled, the user will not be prompted to enter a hostname upon deployment.
6. Click **Next**. It directs you to **Schedule Deployment** option under **Deploy Service** window. Under **Schedule Deployment**, two options are there:
   - **Deploy Now**: To deploy the service immediately, select the option Deploy Now.
   - **Schedule later**: To deploy the service later, select the option Schedule later.

7. Select desired date and time from the **Date and Time** drop-down menu.
8. Click **Finish**.
9. If you have selected **Deploy Now** option after clicking **Finish**, you get a message, stating that; **Are you sure you wish to deploy the service?** Click **Yes** to deploy now.

NOTE: If you want to deploy multiple service on many servers. It is recommended to break these up into smaller group of templates. It is recommended to put 5–10 servers in a single template.

Adding Attachments

You can attach any kind of files to template by using Add Attachment feature. You can attach multiple files.

NOTE: The size limit of attached files is 50 megabytes.

1. Click **Add Attachment** under **Template information** tab, in the right pane of **Template** page. **Add Attachment** window is displayed.
2. You can attach any kind of files to template by using **Add Attachment** feature. You can attach multiple files.
3. Click the **browse** button. Browse file from local file system, click **Open**. It redirects you to **Templates** page. There you can see the newly added file.

NOTE: This operation may take a time based on their size.

4. To view the file, select the attached file. Right-click on it. A window is displayed. There, from the **Open with** drop-down menu, select Notepad. Click **Ok**. A window is displayed, there you can view the file.
5. You can delete the file by clicking the delete icon. After you click delete icon, a window is displayed by stating that **Are you sure that you want to delete this attachment?** Click **Yes** to delete the file.

NOTE: If you try to attach a file with the same name of already attached file, you get an error message. You can attach multiple file with different file name.

Decommissioning services provisioned by ASM

When a service provisioned by ASM is no longer required, it is important to decommission the resources. Therefore, the resources can be provisioned for future services.

The steps to accomplish this task differ based on the type of resource component provisioned. For hosts provisioned by ASM, the default behavior when a service is deleted to turn off the host. For server, extra cleanup is required after turning off the server. For storage provisioned by ASM, the default behavior when a service is deleted to retain the storage volume available to make sure that no critical data is deleted.

As a best practice, you need to perform the following tasks while decommissioning a service. Make sure to perform these tasks to avoid issues in provisioning of future services due to conflicts.

Decommissioning Hyper-V-based storage, host, and clusters

To decommission Hyper-V-based storage, host, and clusters:

1. SCVMM clusters should be uninstalled through SCVMM.
2. SCVMM host groups should be deleted if no longer used.
3. Hyper-V hosts should be removed from SCVMM.
4. Hyper-V hosts should be removed from the domain.
5. Storage volumes should be set offline and deleted when the data is no longer used.
6. If necessary, remove ASM provisioned VLANs from the host facing ports of the switch.
7. Remove host entries from DNS server.

Decommissioning VMware based storage, host, and clusters

To decommission VMware based storage, host, and clusters:

1. Delete unused clusters from VMware vCenter.
2. Delete unused data centers from VMware vCenter.
3. Remove hosts from VMware vCenter.
4. Storage volumes should be set offline and deleted when the data is no longer used.
5. If necessary, remove ASM provisioned VLANs from the host facing ports of the switch.

Component types

The components (physical or virtual or applications) are the main building blocks of a template.

The following component types are defined in ASM:

- Storage
- Switch
- Server
- Cluster
- Virtual Machine
- Application

NOTE: It is recommended to add physical devices to the template first, then configure virtual resources, and lastly configure application settings to be deployed on the resources.

Related links

Storage
Cluster
Virtual Machine
Application

Storage

A **Storage** component refers to the physical storage components that can be added to a template. It is recommended to provision a storage resource first and then configure virtual resources and applications while building a template.

The following storage resource types are provisioned in ASM:

- Compellent
- EqualLogic
- NetApp
- EMC

After selecting **Storage** on the Template Builder page, perform the following actions:

1. In the **Storage Component** dialog box, from the **Select a Component** drop-down list, select one of the storage components:
   - **Compellent**
   - **EqualLogic**
   - **NetApp**
   - **VNX**
2. Under **Related Components**, select the components that you want to map with the selected storage type. For more information about valid component combinations that can be mapped together in a template, see Component Combinations in Templates

3. Click **Continue**.
4. Under **<component name> Storage Settings**, specify the properties for the storage component and click **Add**.

   For more information about the storage settings, see Storage Settings.

Storage settings

Table 3. Storage settings

Field Name	Description
EqualLogic Storage Settings	
Target EqualLogic	Specifies the EqualLogic storage device where the volume is created.
Storage Volume Name	Select the volume in EqualLogic. To create a volume, from the **Storage Volume** drop-down list, select **Create New Volume**.
New volume name	Enter the name of the volume in EqualLogic. A volume is a logical partition in the EqualLogic storage array. The EqualLogic CHAP users have the access to these storage volumes. More than one chap users can have access to the EqualLogic volume.
Storage Pool	Specifies pool name where a volume is. The default storage pool value is *Default*.
Storage Size (e.g. 500 MB, 1 GB)	Specifies the volume size.
Thin Provisioning	Enables thin provisioning on this volume. The possible values are *enable* or *disable*.
Snapshot Reserve %	Refers to the amount of space, as a percentage of the volume size, to reserve for a snapshot.
Thin Min Reserve %	Sets the minimum reserved size for thin provisioned volume configured as percentage of total volume size. This value cannot be less than 10%.
Thin growth Warning %	Sets the warning threshold percentage for thin-provisioned volume. When the thin-reserve reaches this value, a warning message is displayed. The default value is 60%.
Thin growth Maximum %	Sets the maximum growth percentage for thin volume. When thin-reserve reaches this value, the volume is set to offline. The default value is 80%.
Thin warning on Threshold %	Specifies whether a thin provisioning sends an initiator warning when passing the in-use warning threshold.
Thin warning Hard Threshold %	Specifies whether a thin provisioning allows the volume to remain online after reaching the max-growth threshold.
Multihost access of volume	This parameter enables or disables multihost access on a volume. The possible values are *enable* or *disable*.
Authentication	Enables you to select one of the following authentication methods to access the storage volume: · **CHAP** · **IQN/IP** **NOTE: For VMware based deployment, you can use IP or Chap authentication.**
Chap username	Specifies the CHAP username. A valid CHAP username must be less than or equal to 63 alphanumeric characters. The access to CHAP username is limited. **NOTE: The Chap username and Chap secret fields are displayed only if authentication type is selected as Chap.**

Field Name	Description
Chap secret	Specifies the CHAP password. A valid CHAP password must be less than or equal to 254 characters. If the password is not specified, then it is generated automatically.
Initiator IQN or IP Addresses	Specifies the IQN or IP addresses that you want to configure on the EqualLogic storage volume to enable access for the IPs or IQNs. Enter the comma-separated list containing the IP addresses or IQN addresses. The list should not contain a white space. A valid IP address list must be in the format: 172.19.15.2,172.19.15.3,172.19.15.4 A valid IQN address list must be in the format: iqn.2001-05.com.dellsoftware01,iqn.2001-05.com.dellsoftware02,iqn.2001-05.com.dellsoftware01
Compellent Storage Settings	
Target Compellent	Specifies the compellent storage device where the volume is created.
Storage Volume Name	Specifies the name of the volume that is to be created or destroyed.
Storage Size e.g. 100 GB	Specifies the volume size. Enter the number of 512-byte blocks or the total byte size. To specify a total byte size, use k for kilobytes, m for megabytes, g for gigabytes, or t for terabytes.
Boot Volume	Specifies if the mapped volume is designated to be a boot volume.
Volume Folder	Specifies the name of an existing volume folder where a volume is to be created. In case the folder does not exist, a new folder is created.
Purge Volume	This property indicates that the volume must be purged. If the purge option is not specified, the volume is still visible using the volume show command and contains the status of the Recycled. The possible values are *yes* or *no*. The default value is *yes*.
Volume Notes	Specifies the notes for the volume. By default, no notes are included.
Replay Profile	Specifies the replay profiles for the volume.
Storage Profile Name	Specifies the replay profiles for the volume.
Server Notes	Specifies the optional user notes associated with the server.
Operating System Name	Specifies the operating system type, which is set in the Compellent server object of the Compellent storage center.
Server Object Folder	Specifies the folder for the server.
Server WWN Values	Specifies a globally unique World Wide Name (WWN) for the requested HBA.
Port Type	Refers to the transport type for all HBAs being added. This option is required if the manual flag is set. The possible values are *Fibre Channel* and *iSCSI*. For iSCSI Compellent set the port type to iSCSI.
Manual	This parameter sets an optional flag to configure the requested HBAs before the HBAs are discovered. If the WWN matches a known server port, then this flag is ignored. If this flag is present, then the **Port Type** must also be specified. The possible values are *true* or *false*.
Force Map	If the value of this property is defined, it forces mapping, even if the mapping exists. The possible values are *true* or *false*.

Field Name	Description
Map Read Only	Specifies whether a map is read-only. The possible values are *true* or *false*.
Single Path Map	Specifies that only a single local port can be used for mapping. If omitted, all local ports are used for mapping. The possible values are *true* and *false*.
Configure SAN Switch	Enables the zone configuration on the Brocade FC SAN switch.
NetApp Storage Settings	
Target NetApp	Specifies the NetApp storage device where the volume is created.
Storage Volume Name	Select the volume name on the NetApp array. To create a volume, from the **Storage Volume** drop-down list, select **Create New Volume**.
New volume name	Enter the name of the volume that is to be created or destroyed. The storage volume names created on same aggregate must be unique in a NetApp storage array.
Storage Size e.g. 100 GB	Specifies the volume size. Enter the number of 512-byte blocks or the total byte size. You can specify the total byte size in the following formats: MB for megabytes, GB for gigabytes, or TB for terabytes. The volume size must be between 20 MB and 999 TB.
Aggregate Name	Specifies the aggregate name on which the volume is created.
Space reservation mode	Specifies the type of volume that guarantees the new volume uses. Possible values: **none**, **File**, **Volume**. If any value is not selected, the default volume guarantee type is set to **Volume**.
The percentage of space to reserve for snapshots	Specifies the percentage of space to reserve the snapshots. Default value is 0.
Auto increment	Select this check box to enable auto increment of volume size. By default, auto increment is enabled.
Persistent	• In Data ONTAP 7-mode, the persistent is enabled by default. If it is enabled, modify the **etc/exports** file to append the rule for a permanent change. (The new rule still takes effect immediately.). • In Data ONTAP Cluster-Mode, the export entries are always persistent. Persistent is enabled by default. If persistent is not enabled an error occurs.
NFS Target IP	Specifies the interface IP that is used for NFS traffic in your environment.
VNX Storage Settings	
Target VNX	From the **Target VNX** drop-down menu, select the VNX that you want to deploy.
Pool Name	Select the target pool name from the **Pool Name** drop-down menu.
Storage Volume Name	Select the storage volume name from the **Storage Volume Name** drop-down menu.
New Volume Name	To create a volume, from the **Storage Volume Name** drop-down menu, select **Create New Volume**.
Configure SAN Switch	Enables the zone configuration on the Brocade FC SAN switch.
Storage Size e.g. 100 GB	Specify the volume size.
Type	List the LUN types that are supported by storage. **Non Thin** is the default option.

Field Name	Description
	However, you can use **Snap**, **Thin**, and **Compressed** types by separately installing them. For more information on installing plug-ins, see **Installing Plug-ins for EMC to Support Volume Provisioning** section in *Installation Guide*.
Folder Name	Type the folder name.

Server settings

Table 4. Server settings

Options	Description
Select a Component	Select one of the following options from the drop-down menu: · **Server** · **Server (O/S Installation Only)** · **Server (Hardware Only)**
# of Instances	Type the number of the server instances that you want to add.
Associated Resources	Select **Associate All Resources** or **Associate Selected resources** to associate all or specific components to the new component.
Import Configuration from Reference Server	Click this option to import an existing server configuration and use it for the server component settings. On the **Select Reference Server** page, select the server from which you want to import the settings, and click **Select**.
Import from Existing Template	Click this option to import configuration from a server that is part of an existing template. On the **Select Component** page, select the server under a template, and click **Select**.
Upload Server Configuration Profile	Click this option to upload configuration XML file to ASM.
Validate Settings	Click this option to determine which may be chosen for a deployment with this template component.
Hardware Settings	
NOTE: This setting is applicable only for Server and Server (Hardware Only) components.	
Target Boot Device	Specifies the target boot device. The options available are — **Boot from SAN (FC)**, **Local Hard Drive Boot From SAN (iSCSI)**, **None**, **None (With RAID Configuration)**, **SD with RAID enabled**, and **SD with RAID disabled**. **NOTE: The SD with RAID enabled option allows you to boot from the SD and then proceed with creating the RAID virtual disks.**
RAID	You can configure RAID using this feature. The following options are available to configure RAID Level: · **Basic RAID Level** · **Advanced RAID Configuration** **Basic RAID Level**: Select **Basic RAID Level** option, and then select RAID level from the **Basic RAID Level** drop-down menu. ASM supports external and internal RAID controllers using the Advanced RAID Configuration feature. **Advanced RAID Configuration**: If you select Advanced RAID Configuration, You get two buttons **Add Internal Virtual Disks**, **Add**

Options	Description
	External Virtual Disk. There are 4 settings under **Add Internal Virtual Disks**, **Add External Virtual Disk**: • **Virtual Disk**: Lists the ID number of the virtual disk. **NOTE: The operating system is installed on the first virtual disk. Also, you cannot set the first disk to non-RAID mode.** • **RAID Level**: Select RAID level from the drop-down menu. **NOTE: You can also set specific disk to non-RAID mode by selecting Non-RAID level from the RAID Level drop-down menu.** • **# of Disks**: Select number of disks according to the selected RAID level. You may specify "Minimum" or "Exactly" to determine whether ASM should create the virtual disk with the exact number of drives or use as many drives as available. **NOTE: If the number of selected disks is not correct for the chosen RAID level, template validation does not allow you to proceed further.** • **Disk Type**: Select disk type from the drop-down menu. You can select **Any Available**, **First Disks**, **Last/Rear Disks**, **Require HDD**, and **Require SSD** to specify the type of drives to be selected for the virtual disk. A virtual disk cannot be created with a mix of SSD and HDD. There is a feature, **Enable Global Hotspares**. This option is available for both **Add Internal Virtual Disk** and **Add External Virtual Disk**. By using this feature, you can specify number of hot spares you want to set for disk. **NOTE: ASM supports MD1400 and manages MD1400DAS through second RAID Controller. ASM provides the ability to configure a second RAID controller to support the MD 1400 external storage array. To support this, you must have a second PERC device in your system. It is recommended to use the PERC H830 storage controller with the MD 1400.**
Server Pool	Specifies the pool from which servers are selected for the deployment.
BIOS Settings	
NOTE: This setting is applicable only for Server and Server (Hardware Only) components.	
System Profile	Select the system power and performance profile for the server.
User Accessible USB Ports	Enables or disables the user accessible USB ports.
Number of Cores per Processor	Specifies the number of enabled cores per processor.
Virtualization Technology	If this is enabled, the additional hardware capabilities provided by virtualization technology are enabled.
Logical Processor	Each processor core supports up to two logical processors. If enabled, the BIOS reports all logical processors. If disabled, the BIOS reports only one logical processor per core.

Options	Description
Node Interleaving	If the system is configured with matching memory, enables memory node interleaving. If disabled the system supports nonuniform memory architecture memory configurations. **NOTE: Ensure that you disable the Node-Interleave option in the server BIOS when creating a virtual machine on a HyperV server.**
Execute Disable	Enables or disable execute disable memory protection.
OS Settings	
NOTE: This setting is applicable for Server and Server (O/S Installation Only) components.	
Auto-generate Host Name	**Auto generate host name** option is displayed on **Server Component** window for generating host name. If you already auto generated host name on Server Component window, Auto generate host name option will not be display. · If you select the **Auto-generate Host Name** check box, a **Host Name Template** field is displayed. · On **Host Name Template** field, type unique host name for deployment. You must use variable while generating host name. For Example: It can be service tag or Service tag+ Vendor+ Unique number. If you clear **Auto-generate Host Name** check box, **Host Name Template** field is disappeared. **NOTE: Auto- generate Host name feature is applicable for both the server, server(O/S Installation only). If there is multiple instances of deployment, you have to select Auto-generate Host name option.** **NOTE: When you have static assigned IP and if you have DNS configured in template, DNS use the IP to look up the hostname and use it as hostname for the deployment.**
OS Image	Specifies the target repository where the OS image install files are located. The default repositories are ESXi. The additional repositories are shown if the user created them on the ASM appliance. **NOTE: If you select an operating system from the OS Image drop-down menu, the field NTP Server is displayed:.. This is an optional component for all operating systems except Hyper-V, but we highly recommend you to enter an NTP server IP in the field to ensure proper time synchronization with your environment and ASM appliance. Sometimes when time is not properly synchronized, service deployment failure can occur.** **NOTE: If you want to add more than one NTP server in the OS section of a server component, make sure to separate the IP addresses using comma ().** **NOTE: If you select Windows operating system from the OS image drop-down menu, the following fields are displayed:** · **Install HyperV**: Select the check box to install HyperV. · **OS Image Version**: From the drop-down menu, select the OS image version.

Options	Description
Administrator password	Enter the administrator password that set on the installed OS.
Confirm administrator password	Enter to confirm the administrator password.
Select iSCSI Initiator	Select one of the following: • Hardware Initiator • Software Initiator **NOTE: iSCSI Initiator is only supported with VMware.** Also, this option is supported only on the EqualLogic iSCSI storage and Compellent iSCSI storage.
Install EqualLogic MEM	If the value is `True`, install EqualLogic Multipathing Extension Module.
Product Key	Specifies the product key to install the OS image on the server.
Timezone	Specifies the time zone of the server.
NTP Server	Specifies the IP address of the NTP server for time synchronization. If you want to add more than one NTP server in the OS section of a server component, make sure to separate the IP addresses using comma (,).
Language	Specifies the language to be displayed in the installed operating system. That is, Windows operating system.
Keyboard	Specifies the key board language to be used during Windows installation.
Domain Name	Specifies the domain name to which you want to add the host. For example, aidev
FQ Domain Name	Specifies the Fully Qualified Domain Name (FQDN) to which you want to add the host. For example, aidev.com
Domain Admin Username	Specifies the username to access the domain.
Domain Admin Password	Specifies the admin password to add the host to the domain.
Domain Admin Password Confirm	Enables you to reconfirm the admin password to add the host to the domain.
Network Settings	
NOTE: This setting is applicable for Server and Server (Hardware Only) components.	
Add New Interface	Click **Add New Interface** option to create a network interface in a template server component. Under this interface all network settings are specified for a server. This interface is used to find a compatible server in inventory, for example if "Two Port, 10 gigabit" is added to the template, when the template is deployed ASM will match a server which has a two port 10-gigabit network card as it's first interface. For more information on adding a new interface, seeAdding New Interface.
Static Network Default Gateway	Select the default gateway IP address for routing network traffic.

Options	Description
Identity Pool	Select the virtual identity pool from which virtual identities (MAC address and WWPN/WWNN) are selected for boot from SAN deployment.

NOTE: After entering the information about PXE network in the respective field as described in the table above, ASM will untag vLANs entered by the user in the PXE network on the switch server facing port. If there is vMotion and Hypervisor network, for the entered information ASM tags these networks on the switch server-facing ports. If there is Rack Server, ASM configures those vLANs on TOR server facing ports (untag PXE vLANs, and tag other vLANs). In the case for Blade Servers, ASM configures those vLANs on the IOM server facing ports(untag PXE vLANs and tag other vLANs).

NOTE: ASM does not only import basic settings from reference server but also imports all the BIOS settings and advanced RAID configurations from the reference server and allows you to edit the configuration.

For some BIOS settings, they may become not applicable when other BIOS settings are applied. ASM does not correct these setting dependencies. When setting advanced BIOS settings use caution and verify that BIOS settings on the hardware are applicable when not choosing "Not Applicable" as an option. For example, when disabling SD card the settings for "Internal SD Card Redundancy" becomes not applicable.

NOTE: You can edit any of the settings visible in the template, but many settings are hidden when using this option. For example there are only 10 of the many BIOS settings that you can see and edit using template but All BIOS settings can be configured so if you want to edit any of those settings that we don't get to see through template, you should edit them prior to importing or uploading the file.

NOTE: The preceding note is applicable for Import Configuration from Reference Server, Import from Existing Template, Select Reference Server.

NOTE: Validate settings shows which potential servers in inventory are compatible with the component configuration in the template.

Adding New Interface

Under **Network Settings**, perform the following settings:

NOTE: Add New Interface is used to create a network interface to match to a network card on the server when deploying a template.

1. On the **server component** page, under **Network Settings,** click **Add New Interface**. A new interface section is displayed.

   NOTE: Add new interface feature is used to create an interface to match with the interface on the server before deploying a template

2. Enter the following information for the new interface:

   - **Fabric Type** — Select either any of the following options; **Ethernet (NIC/CAN)** or **Fibre Channel (HBA)**.
   - **Port Layout** — Select the NIC type from the drop-down menu.
   - **Partitioning** — Select the **Enable Partitioning Ports (NPAR)** option to enable port partitioning.

     NOTE: This option is not selected by default.

   - **Redundancy** — Select the **Duplicate port settings and configure teaming** to enable duplicating port to create redundancy.

     NOTE: This option is not selected by default.

3. Enter the following information for each port or partition:

   - **Networks (vLAN)** — Select the available network to use for data transmission.

If you want to use static IP range, you can select old PXE DHCP network option or you can select Lab OS Installation which is a static network.

NOTE: When the OS Installation network is set to Static, OS Installation is supported only for installing Linux, ESXi, and Windows on bare-metal systems with Intel NICs.

- Enter the Minimum and Maximum Bandwidth in percentage.

NOTE: If you select the same network on multiple interface ports or partitions, ASM performs the following:

- On systems with Windows and ESXi operating system, a team or bond is created in the operating system to enable redundancy.
- On systems with Red Hat, CentOS, and SUSE Linux operating system:
  - LACP-enabled (mode 4 or 802.3ad) bond is created in the operating system.
  - LACP enabled port-channel is created on the server-facing ports of the switch to which the server is connected. The port-channel selected is automatically assigned to the lowest port available in the connected switch.
  - The MTU value is set to either 1500 or 9000.
  - After the server tears down, all the above listed configurations are removed.

NOTE: Ensure that lacp ungroup is not set to vlt on your switches.

NOTE: The MTU value is set to either 1500 or 9000 based on user selection in the template.

Server (OS Installation only) Component Settings

On **Getting Starte**d page, click **Publish Template**. On **Template** page, click **Create Template**. On Create Template page:

Template Name field: Enter Template name in the **Template Name** field.

Template Category: Select category of template from the **Template Category** drop-down menu.

Click **Save**, it directs you to **Template Builder** page. On the **Template Builder** page, click **Add Server**. It directs you to Server Component window. From the **Select a Component** drop-down menu, select **Server (O/S Installation only)**. After that **# of Instances** drop-down menu is displayed. From the **# of Instances** drop-down menu, select the number of the server instances that you want to add, after that click **Continue**. Under **OS Settings**, few fields, drop-down menu and check box are displayed. These all are listed here:

- **Auto-generate Host Name**
- **Host Name Template**
- **OS Image**
- **Administrator password**
- **Confirm administrator password**
- **Time Zone**
- **NTP Server**
- **Server Pool**

Auto-generate Host Name:

If you select the **Auto-generate Host Name** check box, a **Host Name Template** field is displayed. You must use this variable while generating a host name. For Example, a hostname template must start with a letter. The variable portion of the hostname template can be designated to use a service tag or a number to ensure uniqueness. The template may also include a variable for the model or vendor of the server if information about these values is available. It can be service tag or Service tag+ Vendor+ Unique number. If you clear the **Auto-generate Host Name** check box, **Host Name Template** field disappears.

NOTE: Auto-generate Host name feature is applicable for both the server, server(O/S Installation only). If there are multiple instances of deployment, you have to select Auto-generate Host name.

OS Image:

From the **OS Image** drop-down menu, select OS Image.

Administrator password:

Enter your administrator password.

Confirm administrator password:

Reenter your administrator password to confirm password.

Timezone:

After you select OS Image Type, **Timezone** and **NTP Server** fields are displayed. Select time zone from the **Timezone** drop-down menu.

NTP Server:

This is an optional component for all operating systems except Hyper-V. You can specify NTP server for bare metal OS installation, ESXi installation.

NOTE: It is recommended to enter an IP address in the NTP Server field as sometimes when there is not time synchronization with environment a service deployment may fail.

Server Pool:

Enter the server pool name in the Server Pool field. Click **Add**. It directs you to **Template Builder** page. There you can see the newly added template. This template is used only for deploying Operating System on server.

NOTE: Here you will not get any option for Hardware, BIOS, and network configuration. You are required to check that manually weather or not server has hard disks available and network is configured on rack switch or blade chassis.

Importing from existing template

The **Importing From Existing Template** feature enables you to import configuration from a server which is already there is an existing template. You can edit the settings after importing the configuration from existing template.

To import a configuration from a server which is already part of an existing template, perform the following tasks:

1. On the **Server Component Settings** page, click **Import from Existing Template**.
2. On the **Select Component** page, select a server under a template to import the configuration.
3. Click **Select**.

   It imports the configuration from existing template.

Uploading Server Configuration Profile

The **Upload Server Configuration Profile** feature enables you to upload configuration XML file to ASM. To upload a configuration XML file to ASM, perform the following tasks:

1. Click **Upload Server Configuration Profile**. **Upload Server Configuration Profile** window is displayed.
2. On the **Upload Server Configuration Profile** window, click **Browse**.
3. Select a file what you want to upload, click **Open**.
4. Click **Continue** on **Upload Server Configuration Profile** window.
5. After performing all the above steps click **Save**.

The settings uploaded from the configuration XML file are applied to the hardware configuration of the target server at deployment time.

Cluster

After selecting **Cluster** on the template builder page, perform the following actions:

1. In the **Cluster Component** dialog box, from the **Select a Component** drop-down list, select one of the following options:
   - **VMWare**
   - **Hyper-V**
2. In the **# of Instances** box, enter the number of cluster instances.
3. Under **Related Components**, select the components that you want to map with the selected cluster instance. For more information about valid component combinations that can be mapped together in a template, see Component Combinations in Templates
4. Click **Continue**.
5. Under **Cluster Settings**, specify the settings that you want to configure on the cluster components and click **Add**.

   For more information about the cluster settings, see Cluster Component Settings

Cluster component settings

Table 5. Cluster component settings

Field Name	Description
Cluster Settings (Target vCenter)	
Target Virtual Machine Manager	Select virtual machine manager from the **Target Virtual Machine Manager** drop-down menu.
Data Center Name	Select data center name from **Data Center Name** drop-down menu.
Cluster Name	Select new cluster name from **Cluster Name** drop-down menu.
New cluster name	Select new cluster name from **New Cluster Name** drop-down menu.
Cluster HA Enabled	Enables or disables highly available cluster. You can either select or clear the check box. By default, it is unchecked.
Cluster DRS Enabled	Enables or disables distributed resource scheduler (DRS). You can either select or clear the check box. By default, it is unchecked.
Storage DRS Enabled	Enables or disables the storage DRS. If you select the **Storage DRS Enabled** check box, configure the following: • Type storage cluster POD name in the **Storage Cluster Name** field. • Select the volumes to **Data stores to Add to Cluster**.
Switch Type	Allows you to configure the virtual switches as distributed or standard for the host network. If enabled, the switches are configured as distributed switches. **NOTE: This option is applicable only for VMware clusters.** **NOTE: Ensure that version of the distributed switches that are configured is based on the lowest available host version in a cluster to ensure compatibility with all the clusters in the host.**
Cluster Settings (Target Hyper-V)	
Hypervisor Management Software	Specifies the target SCVMM.
Host Group	Specifies the host group that you want to target.

Field Name	Description
New host group name	Enables to specify a new host group. Enter the host group in the format: All hosts\ <group name>
Cluster Name	Specifies the name of the cluster.
New cluster name	Enables you to specify a new cluster.
Cluster IP Address	Specifies the cluster IP address.

Virtual Machine

A **Virtual Machine** is configured on top of a cluster, while building a template.

After selecting the **Virtual Machine** component on the **Template Builder** page, perform the following actions:

1. In the **Virtual Machine Component** dialog box, from the **Select a Component** drop-down list, select one of the following:
   - **vCenter Virtual Machine**
   - **Clone vCenter Virtual Machine**
   - **Clone Hyper-V Virtual Machine**
2. In the **# of Instances** box, enter the number virtual machine instances that you want to configure.
3. Under **Related Components**, select the components that you want to map with the virtual machine instance. For more information about valid component combinations that can be mapped together in a template, see Component Combinations in Templates.
4. Click **Continue**.
5. Under **Virtual Machine Settings**, specify the settings that you want to configure on the virtual machines and click **Add**.

   For more information about the virtual machine settings, see Virtual Machine Settings.

Virtual machine settings

Table 6. Virtual machine settings

Virtual Machine Component	
Field Name	**Description**
vCenter Virtual Machine	
Virtual Machine OS Settings	
Auto-generate Host Name	Select to generate a new name for each virtual machine. **NOTE: The Host Name Template field is displayed if this option is selected.**
Host Name Template	Displays the naming convention followed for the virtual machines deployed in a service. **NOTE: The naming convention that is followed consists of vm${num), where *vm* indicates a static text that you can provide and *${num}* is a variable number that is enumerated for the number of virtual machines that you create. For example, if you deploy a service with 3 virtual machines and if you select the auto-generate option and provide the name as vm, the virtual machines are named as vm1, vm2, and vm3.**
Administrator password	Specify OS administrator password that is set on the installed OS.
Confirm administrator password	Enter the password to confirm the administrator password.

Virtual Machine Component	
Field Name	**Description**
OS Image	Specifies the target repository where the OS image install files are located. The default repositories are ESXi. The additional repositories are shown if the user created them on the ASM appliance.
NTP Server	Type the IP address of the NTP server for time synchronization. If you want to add more than one NTP server in the OS section of a server component, make sure to separate the IP addresses using comma (,).
Virtual Machine Settings (**vCenter Virtual Machine**)	
Number of CPUs	Indicates the number of CPUs specified while configuring a Virtual Machine.
Virtual Disk(s)	Specifies the size to allocate for virtual machine hard disk. The default size is 32 GB. **NOTE: The operating system is installed on the first virtual disk.**
Add Virtual Disk	Click this option to create extra virtual disks.
Memory in MB	Indicates the memory specified while configuring a virtual machine.
Networks	Allows you to set the virtual machine network or set static networks already created in ASM as workload networks for the virtual machines. **NOTE: Static IPs are applicable only for vCenter Virtual Machine on which you are installing Linux operating system.**
Static Network Default Gateway	Set the default gateway for the static network selected. **NOTE: This option is applicable only if you have set the Networks setting to a static network.**
Virtual Machine Settings (**Clone vCenter Virtual Machine**)	
Auto-generate Name	Select to generate a new name for each virtual machine.
VM Name Template	Displays the naming convention followed for the virtual machines deployed in a service. **NOTE: The naming convention that is followed consists of vm${num), where *vm* indicates a static text that you can provide and *${num}* is a variable number that is enumerated for the number of virtual machines that you create. For example, if you deploy a service with 3 virtual machines and if you select the auto-generate option and provide the name as vm, the virtual machines are named as vm1, vm2, and vm3.**
Clone Type	Select the clone type from **Clone Type** drop-down menu.
Source	Specifies the name of the source template.
Source Datacenter	Specifies the VMware data center where the source template or virtual machine resides.
VM Guest Customization Spec	Select the specs available in vCenter inventory. **NOTE: To make these specs available for selection, update the vCenter inventory with customized spec. For more information, see Creating customization specification for vCenter virtual machine clone.**
Number of CPUs	Indicates the number of CPUs specified while configuring a Virtual Machine.

Virtual Machine Component	
Field Name	**Description**
Virtual Disk Size (GB)	Specifies the size to allocate for virtual machine hard disk.
Memory in MB	Indicates the memory specified in GB while configuring a Virtual Machine.
Networks	Allows you to set the virtual machine network or set static networks already created in ASM as workload networks for the virtual machines. **NOTE: Static IPs are applicable only for vCenter Virtual Machine on which you are installing Linux operating system.**
Static Network Default Gateway	Set the default gateway for the static network selected. **NOTE: This option is applicable only if you have set the Networks setting to a static network.**
Virtual Machine Settings (**Clone Hyper-V Virtual Machine**)	
Auto-generate Name	Select to generate a new name for each virtual machine. **NOTE: If this option is selected, the VM Name Template field is displayed.**
VM Name Template	Displays the naming convention followed for the virtual machines deployed in a service. **NOTE: The naming convention that is followed consists of vm${num), where *vm* indicates a static text that you can provide and *${num}* is a variable number that is enumerated for the number of virtual machines that you create. For example, if you deploy a service with 3 virtual machines and if you select the auto-generate option and provide the name as vm, the virtual machines are named as vm1, vm2, and vm3.**
Description	Indicates the number of CPUs specified while configuring a Virtual Machine.
Name	Specifies the size to allocate for virtual machine hard disk.
Template	Specifies the SCVMM virtual machine template name.
Path	Specifies the storage path where VM clone is deployed.
Networks	Specifies the ASM networks, which are connected to the virtual machine clone.
Block Dynamic Optimization	If it is `True`, the block dynamic optimization is enabled. Possible values: `True` or `False`.
Highly Available	Enables whether the VM is a highly available VM.
Number of CPUs	Specifies the Number of CPUs to allocate to the virtual machine.
Memory in MB	Specifies the memory to allocate to the virtual machine.
Start Action	Selects the action to perform automatically when the virtualization server starts.
Stop Action	Selects the action to perform when the virtualization server stops.

Deploying customization specification for vCenter virtual machine clone

You can apply customization specification to virtual machines deployed using ASM. A customization spec allows you to create a spec with settings such as host name, domain name, network settings, static IPs that can be applied to VM clones. Before deploying

a customization spec, ensure that you have created a spec and added it to the vCenter inventory. For more information on creating a customization spec, see Creating customization specification for vCenter virtual machine clone.

NOTE: Customization specification only applies to VMware virtual machine clone.

To deploy customization specification for vCenter virtual machine clone:

1. Click **Templates**.
2. Create and edit the template. For more information on creating a template, seeCreating template.
3. On the **Template Builder** page, click **Add VM**.
   The **Virtual Machine Component** window is displayed.
4. Select **Clone vCenter Virtual Machine** from the **Select a Component** drop-down menu.
5. Under the **Associated Resources** section, select **Associate Selected Resources** to associate all or specific components to the new component.
6. Click **Continue**.
7. Under **Virtual Machine Settings**, select or enter all the parameters. For more information on Virtual Machine Settings, see Virtual Machine Settings.
8. To apply the settings and deploy the customization specification, click **Add**.

Creating customization specification for vCenter virtual machine clone

To create customization specification:

1. Log in to **vCenter**.
2. Click **Inventory Management Customization Specification Manager**.
3. Enter the settings such as host name, domain name, time zone, and network.
4. Click **Finish**.

Application

The **Application** component is configured on top of virtual resources in ASM. However, an application component can be installed on a physical server that has a non-ESXi OS and non-Hyper-V OS.

ASM provisions multiple applications for deployment.

After selecting **Application** component on the template builder page, perform the following actions:

1. In the **Application Component** dialog box, from the **Select a Component** drop-down list, select the application that you want to configure on the virtual machines.
2. In the **# of Instances** box, enter the number of application instances.
3. Under **Related Components**, select the components that you want to map with the application instance. For more information about valid component combinations that can be mapped together in a template, see Component Combinations in Templates
4. Click **Continue**.

   Based on your application select, the page displays the application properties for you to configure.
5. Under **Application Settings**, specify the application properties.

   See Application Components Settings.
6. Click **Add**.

Adding application

To add application to a template:

1. Click **Templates**.
2. Select the template you want to edit and click **Edit** on the right pane.
   The template details page is displayed.

3. Click **Add Application**.
   The **Add Application** window with the list of resources available in the template is displayed.
4. Select the resources to which you want to add the application and click **Next**.

   NOTE: You can select only supported for physical or bare metal servers, or non-hypervisor servers, or virtual machines.
5. From the **Add Application** drop-down menu, select any one of the following default application types and click **Add**:
   - **windows_postinstall**
   - **citrix_d7**
   - **mssql2012**
   - **linux_postinstall**

   NOTE: The custom modules created using add-on modules are also displayed in the Add Application drop-down list.

   NOTE: You can add multiple applications to a resource. Also, you can arrange the application in order by clicking the arrows beside the resource.

   NOTE: You must add an application for each component by selecting the resource individually. Adding application on one resource does not reflect the same on another resource.

   NOTE: To modify existing applications, you can click back in the application box and edit applications.
6. Click **Next**.
   The **Applications Settings** window is displayed.
7. Type the required information and click **Finish**.
   A confirmation prompt with the following message is displayed — **Are you sure you want to finish configuration?**
8. Click **Yes** to confirm.
   On the template details page, an application icon appears on the resource to which the application was added.

   You can click the application icon on the resource to view the list of applications, edit, or delete applications.

VMware vSAN

VMware vSAN storage feature allows to create resource pools of a local storage space from multiple ESXi host.

NOTE: Before creating the VMware vSAN template, ensure that you have a static network of type VSAN defined.

For server component settings:

1. On the home page, click **Templates**.
2. On the **Templates** page, create a vSAN template.
3. On the **Template Builder** page, click server component, and then click **Edit**.
   The **Server Component** page is displayed.
4. Click **Continue**.
5. Under **OS Settings**, select the **Configure local storage for VMware vSAN** check box.
6. Under **Hardware settings**, select **SD with RAID enabled for VMware vSAN** or **Local Disk For VMware vSAN** from the **Target Boot Device** drop-down menu.

   NOTE: The Local Disk for VMware vSAN option is applicable for servers with SATA AHCI controller and physical disks installed in the back panel.

   NOTE: To fully support vSAN, it is recommended to use ESXi 6.0 update 2 or later. To determine the version of ESXi 6.0 which ships with your version of Active System Manager, see *Compatibility Matrix*.

   For more information on the OS Settings and Hardware Settings, seeServer settings.
7. Under **Network Settings**, clear the **Enable Partitioning Ports** check box, you can add VLAN for networks — Hypervisor Management, Hypervisor Migration, OS Installation, and Public or Private LAN on the same partition.
8. Create another interface, clear the **Enable Partitioning Ports** check box, add the VSAN VLAN and select the redundancy check box.

For more information on the Network Settings, seeServer settings.

For cluster component settings:

Table 7. Cluster component settings

Options	Descriptions
Target Virtual Machine Manager	Select virtual machine manager from the **Target Virtual Machine Manager** drop-down menu.
Data Center Name	Select data center name from **Data Center Name** drop-down menu.
New Data Center	Type the new data center name in the **New Data Center** box.
Cluster Name	Select new cluster name from **Cluster Name** drop-down menu.
New cluster name	Type new cluster name in the New cluster name in the New cluster name box.
Switch Type	Select the switch type as **Distributed**.
Cluster HA Enabled	Enables or disables highly available cluster. You can either select or clear the check box. By default, it is unchecked.
Cluster DRS Enabled	Enables or disables distributed resource scheduler (DRS). You can either select or clear the check box. By default, it is unchecked.
Enable VMware vSAN	Select the **Enable VMware vSAN** check box.

vSphere VDS Settings

Under **vSphere VDS Settings**, create appropriate network type such as Hypervisor Management, Hypervisor Migration, OS Installation, and Public or Private LAN.

Application component settings

Table 8. Application component settings

Field Name	Description	Default and Possible Values
Mssql 2012		
Media	Specifies the location of the SQL install image.	Default value: **D:**
instancename	Specifies a SQL Server instance name for the instance that is being completed. For named instance enter a user-specific name.	Default value: `MSSQLSERVER`
features	Specify the list of individual SQL server components to install.	Default values: `SQLENGINE,CONN,SSMS,ADV_SSMS` Possible values: `Replication, FullText, DQ, AS, RS, DQC, IS, MDS, BC, BOL, BIDS,`

Field Name	Description	Default and Possible Values
		DREPLAY_CTLR, DREPLAY_CLT, SNAC_SDT, SDK, LocalDB
sapwd	Specifies the password for SQL Server SA Account.	
agtsvcaccount	Specifies the account for the SQL Server Agent service.	Default value: NT SERVICE \MSSQLSERVER
agtsvcpassword	Specifies the password for SQL Server Agent service account.	Password is not required for NT service accounts.
assvcaccount	Specifies the account for the Analysis Services service.	Default value: NT SERVICE \MSSQLSERVER
assvcpassword	Specifies the password for the Analysis Services service.	Password is not required for NT Service accounts.
rssvcaccount	Specifies the startup account for Reporting Services.	Default value: NT SERVICE \MSSQLSERVER
rssvcpassword	Specifies the password for the startup account for Reporting Services service.	Password is not required for NT Service accounts.
sqlsvcaccount	Specifies the startup account for the SQL Server service.	Default value: NT SERVICE \MSSQLSERVER
sqlsvcpassword	Specifies the password for SQLSVCACCOUNT.	Password is not required for NT Service accounts.
instancedir	Specifies a non-default installation directory for shared components.	Default value: C:\Program Files \Microsoft SQL Server\\
ascollation	Specifies the collation setting for Analysis Services.	Default value: Latin1_General_CI_AS
sqlcollation	Specifies the collation settings for SQL Server.	Default value: SQL_Latin1_General_CP1_CI_AS
admin	Specifies the administrator account name	Default value: Administrator
netfxsource	Specifies the .Net install file.	
Citrix_xd7		
Source	Specifies the installation media location	Example, if repository created on appliance repo-store directory. "//<ASM appliance IP>/razor/XenDesktop7/x64/XenDesktopSetup"
SQL Server	If the value is True, installs SQL Server component from Citrix installer on the virtual machine to which the component is related.	Possible values: True or False
Delivery Controller	If the value is true, installs Citrix Delivery Controller component from Citrix installer on the virtual machine to which the component is related.	Possible values: True or False

Field Name	Description	Default and Possible Values
Citrix Studio	If the value is true, installs Citrix Studio component from Citrix installer on the virtual machine to which the component is related.	`Possible values: True or False`
License Server	If the value is true, installs Citrix License Server component from Citrix installer onto the virtual machine to which the component is related.	`Possible values: True or False`
Citrix Director	If the value is true, installs Citrix Director component from Citrix installer on the virtual machine to which the component is related.	`Possible values: True or False`
StoreFront	If the value is true, installs Citrix StoreFront component from Citrix installer on the virtual machine to which the component is related.	`Possible values: True or False`
Linux_postinstall		
Install Packages	Optional. Specify a comma-separated list of yum packages (without spaces) to install.	For example: `openssl,mysql,ntp`
Upload Share	Optional. Specifies the share to use for uploading file to server. Share folder must exist.	Default value: **\\myshareserver \folder**
Upload File	Optional. Specifies the file to upload from the share that you have specified.	For example: **install.sh**
Upload Recursive	Determines whether or not to upload all contents of the directory on the share. (For use in optional upload file/script)	Possible values: `True` or `False`
Execute File Command	Optional. Specifies the command to execute uploaded file. The command must be used with upload file present.	
Proxy	Optional. Specifies the proxy to use for yum installs.	For example: **http://proxy:80**
Windows_postinstall		
Share	Optional. Specifies the share to use for uploading file to server. Share folder must be available.	**\\myshareservcer\AppAssureClient**
Install Command	Specifies the command to install executable located on the share.	`Agent-Web.exe /silent reboot=never`
Upload File	Specifies the file to upload from the share that you have specified. Upload File depends on Share. You must upload file to share.	Possible value: **myfile.bat**
Upload Recurse	Determines whether to upload all contents of the directory on the share.	Possible value: `True` or `False`
Execute File Command	Optional. Specifies the command to execute uploaded file. The command must be used with upload file present.	Possible value: **myfile.bat –u username –p password**

Component combinations in templates

In the Template Builder and within a template, there are few components that can be selected and specified, as discussed in the previous sections. However, only certain combinations of these components can logically be used together. The following table

provides information about the valid component combinations supported for template creation. In each vertical column of the table, an X indicates the set of components that can be used together in the same template. For example, reading from the left, a template may contain the following component combinations:

- Storage only
- Storage and Server
- Storage, Server, and Cluster
- Storage, Server, Cluster, and Virtual Machine
- Storage, Server, Cluster, Virtual Machine, and Application
- Server only
- Server and Application
- Cluster only
- Cluster and Virtual Machine
- Cluster, Virtual Machine, and Application
- Server, Cluster, and Virtual Machine

Table 9. Valid template Combinations in templates

Application				x		x			x		
Virtual Machine			x	x				x	x		x
Cluster		x	x	x		x	x	x	x		x
Server		x	x	x	x						x
Storage	x	x	x	x							

NOTE: X's in column indicate components that can be used together in a template

Additional template information

This section provides more details, including pre-requisites, for creating or deploying certain types of templates.

Deploying ESXi cluster for SAN applications

NOTE: This feature is supported only in ASM, version 7.5.1 and later.

When planning to deploy ESXi clusters for SAN applications using Dell Compellent Storage and Brocade SAN switch 6510, there are certain prerequisites to consider, and guidelines that should be followed when creating a template, deploying a service, and cleaning up deployments.

Related links

ESXi cluster deployment pre-requisites
Creating template for ESXi cluster deployment
Deploying service on ESXi clusters
Cleaning up ESXi cluster deployments

ESXi cluster deployment pre-requisites

Before utilizing this ASM solution to deploy ESXi cluster using Dell Compellent storage and Brocade 6510 SAN switch, make sure that the pre-requisites listed in the following table are met.

Table 10. ESXi cluster deployment pre-requisites

Specification	Pre-requisite
Chassis IOM Configuration (if blade use case)	Make sure that the SAN IOM is in access gateway mode.
Managed Rack or Blade Servers Configuration	Make sure that the QLogic FC Adapters installed in any slot for rack servers or fabric B or C for blade servers. ASM queries for WWPN values on a QLogic QME or QLE 2662 or 2572 adapter.
Brocade Switch Configuration	• Create fault domain on Brocade switches for Compellent. • Create both physical and logical ports of the Compellent array. • Make sure active zone set is configured on the Brocade SAN switches.
Compellent Storage Configuration	Must be configured
Resource Discovery	Make sure the following resources are discovered in ASM. • FC Servers for Deployment • FC SAN Brocade Switch • FC IOMs (Optional) • Dell Compellent Storage • VMware vCenter

Creating template for ESXi cluster deployment

Create a template with the following settings to deploy ESXi cluster using Dell Compellent storage and Brocade 6510 SAN switch.

- In the **Template Builder** page, add the following resources by clicking the corresponding components icons.
  - Storage
  - Server
  - Cluster
- To configure Brocade switches, perform the following actions:
  a. In the Storage, click the corresponding storage component icon.
  b. In the **Storage Component** pane, under **Compellent Storage Settings**, set the value as `true` for **Configure SAN Flag** parameter.
- The parameter **iSCSI network** is not required when deploying Fibre Channel storage. If this setting is included, it is ignored.

Related links

Creating template
Building template overview
Building and publishing template

Deploying service on ESXi clusters

On the **Templates** page, select the template created for this use case and click **Deploy Service**.

ASM performs the following actions when you deploy this service:

- Identifies the necessary servers from the FC server pool specified.
- Boots the server when if it is turned on and verifies the FC connectivity.

- Creates the storage volume and server objects that contain the WWPNs on Compellent storage. ASM creates the storage volume and server objects with the names specified in the template.
- If **Configure SAN Switch** parameter is set to true, ASM performs the following actions:
  - Identifies the fault domain of the Compellent storage created on the Brocade switches.
  - Configures the Brocade switch by creating a zone for the server including the WWPN of the FC adapters and the Compellent storage. The zones are added to the active zone set.
- Maps the server object to the Compellent volume.
- Installs ESXi, creates virtual networking based on the template, and creates and formats the VMFS data store for the attached Compellent volume and configures multipathing settings.

Related links

Creating template
Building template overview
Building and publishing template
Deploying service

Cleaning up ESXi cluster deployments

If you delete the service, ASM turns off the ESXi hosts but will not delete any of the objects or connectivity created by the deployment.

You need to determine what infrastructure that you want to retain, and delete any unnecessary Compellent volumes and server objects, Brocade zones, and VMware vCenter objects.

7

Resources

The chassis, servers, switches, storage groups, VMware vCenters, and Microsoft virtualization environments that you can manage using ASM are called resources.

The **Resources** page displays detailed information about all the resources and the server pools that ASM has discovered and inventoried, and allows you to perform various operations from the **All Resources** and **Server Pools** tabs.

NOTE: It may take few minutes to display the discovered resources every time you run the inventory, depending upon the number of resources.

The **All Resources** tab displays the following information, in tabular format, about the resources discovered and managed in ASM.

Table 11. Resources

Field name	Description
Health	Indicates the health of the resources. For more information on the resource state, see Resource health status.
Compliance	Indicates the firmware and software compliance state of the resources. The values displayed are **Compliant**, **Non-compliant**, **Update required**, and **Update failed**. For more information on the compliance status, see Resource firmware compliance status. **NOTE: You can click on the compliance status and view the compliance report.**
OS Hostname	Indicates the host name of the resources.
Resource Name	Indicates the resource name of the resources.
IP Address	Indicates the IP address of the resource. Click the IP address to open the **Element Manager**.
Asset/Service Tag	Indicates the Service Tag of the resources.
Deployment Status	Indicates the deployment status of the resources. The values displayed are **In Use**, **Not in use**, **Available**, **Updating resource**, and **Pending Updates**. **NOTE: You can click on the deployment status and view the service details**
Managed State	Indicates the state of the resources.
Manufacturer/Model	Indicates the manufacturer name and model number of the resources. For example, Dell PowerEdge T630.

To filter resources based on the resource type, click **Show Filter** on the **Resource** page and then select one of the following resource types from **Resource Type** drop-down list:

- **All**
- **Dell Chassis**
- **Element Manager**
- **Servers**
- **Switches**
- **Storage**
- **VM Manager**

Click **Health** to filter the resources based on the following resource health status:

- **All**
- **Healthy**
- **Warning**
- **Critical**

Click the **Managed State** option to filter the resources based on the resource state. The options available are **Managed**, **Unmanaged**, and **Reserved**.

On the **Resources** page, you can also:

- Click **Discover** to discover new resources. For more information on discovering the new resources, see Discovering resources.
- Click **Remove** to remove the resource from ASM. For more information on removing the resources, see Removing resources.
- Click **Export All** to export all the resource details to .csv file.
- To manually run the inventory operation on a resource and update ASM with the latest resource details, select a resource and click **Update Inventory**.
- Select one or more resources and click **Update Resources** to update the firmware and software of the resources.
- Select one or more chassis from the list, and click **Configure Chassis** to configure the basic settings on the chassis.
- On the right pane, you can perform the following actions:
  - Click **View Details** to view the detailed information about the resource.
  - Under **Details**, click the link corresponding to **Firmware/Software compliance** to view the firmware and software compliance report.

Related links

Port View
Understanding server pools

Resource health status

ASM assigns health status to the resources based on the conditions described in the following table.

Table 12. Resource health status

Icon	Health Status	Description
	Healthy	Indicates that there is no issue with the resource and working as expected.
	Warning	Indicates that the resource is in a state that requires corrective action, but does not affect overall system health. For example, the firmware running on the resource is not at the required level or not compliant.

Icon	Health Status	Description
	**Critical**	Indicates that there is an issue in one of the following hardware or software components in the device. Needs immediate attention. • Battery • CPU • Fans • Power Supply • Storage Devices • Licensing
	**Unknown**	Indicates that the state of the resource is unknown.

Resource operational state

After initiating the resource discovery, ASM assigns one or more of the following states to the resources. These operational states display in the **State** columns of the **All Resources** tab on the **Resources** page.

Table 13. Resource operational state

State	Description
Not In Use	Resource is available for deployment.
Deploying	Resource is in the process of being deployed in a service.
Deployed	Resource is deployed in a service.
Pending	One or more of the following tasks are in progress: • Discovering resource. • Determining resource details, including firmware version. • Applying template to the resource. • Updating firmware. • Removing resource from ASM inventory.
Error	Service deployment is failed.
Reserved	Indicates that the ASM only manages the firmware on that particular server, but that server cannot be used for deployments.
Unmanaged	Resource is not managed by ASM.

Port View

You can use the port view feature to view network and Fibre channel connectivity for a particular server.
Perform the following steps to view the port view details:

1. On the home page, click **Resources**.
2. Select a server that is in a **Deployed** state and click **View Details** on the right pane.
   The **Resource Details** page is displayed.
3. Click **Port View**.
   The following information is displayed on the Port View page:

- Topology information for all networks and VLANs deployed in a service.
- Network connections between the devices.
- Health of the resources. For more information, seeResource health status.
- Connection Details section with detailed information on the network devices.
- Zone and zone configuration in the **VLAN-Networks** list for the FC connectivity.

NOTE: If you select a server that is not in a deployed state, only the interface card information is displayed.

To view device details such as host name, model name, and management IP address, or information on associated devices, click the specific ports or devices. For example, to view the VLANs associated with specific partitions, click the partition to view the detail.

NOTE: To view information on intermediate devices in Port View, ensure that the devices are discovered and available in the inventory.

To filter the information based on the connectivity, select an option from the **Display Connections** drop-down menu.

NOTE: The Show All Connections is the default option.

Resource firmware compliance status

Based on the resource firmware compliance with the default repository catalog set, ASM assigns one of the following firmware statuses to the resources.

Table 14. Resource firmware compliance status

Firmware Status	Description
Compliant	The firmware running on the resource is compliant with the firmware version specified in the default catalog.
Non–Compliant	The firmware running on the resource is less than or greater than the firmware version specified in the default catalog. Indicates that firmware update is required.
Update Required	The firmware running on the resource is less than the minimum firmware version recommended in the ASM catalog. Indicates that firmware update is required.

Updating firmware

You can update the firmware of one or more servers that are not compliant with ASM or not to the minimum recommended level:

1. On the home page, click **Resources**, and then click **Update Resources**.
2. On the **Apply Server Firmware Updates** page, select one of the following options:
   - **Update Now** — Select this option to update the firmware immediately.

     ASM applies the firmware updates immediately and then reboot to all servers within this service. For servers belonging to a VMware vSphere cluster, servers will be updated one at a time by putting it first into maintenance mode, then performing the firmware update and rebooting the server, and finally bringing the server out of maintenance mode before moving on to the next server.
   - **Apply Updates on Next Reboot** — Select the option to update the firmware at the next server reboot. ASM stages the firmware update to each server selected until reboot.

     ASM stages the firmware update to each server selected. The update will take effect at the next server reboot.

- **Schedule Update** — Select this option and then select the date and time to update the firmware.

  ASM applies the firmware updates at a selected date and time and then reboot to all servers within this service. For servers belonging to a VMware vSphere cluster, servers will be updated one at a time by putting it first into maintenance mode, then performing the firmware update and rebooting the server, and finally bringing the server out of maintenance mode before moving on to the next server.

3. Click **Save**.

NOTE: Firmware update on a server that is part of a cluster is successful only if the server is set in maintenance mode. ASM sets servers in a cluster in maintenance mode before updating firmware. To ensure that the server remains in maintenance mode, ensure that there are other servers available in the cluster to host the virtual machines of the server that is updated.

NOTE: Firmware update on a VMware cluster is successful only if the cluster is properly configured for HA. For example, the host system can be set in maintenance mode and the virtual machines can be moved from one host to another in the cluster.

Removing resources

NOTE: Only the user with Administrator role can remove resources from ASM.

To remove any particular resource from ASM, perform the following steps:

1. On the home page, click **Resources**.
2. On the **Resources** page, click the **All Resources** tab.
3. From the list of resources, select one or more resources, and click **Remove**.
4. Click **OK** when the confirmation message is displayed.

If you remove a Chassis, the Chassis and associated servers and I/O modules are removed from ASM. The removal process shuts down the servers and erases identity information to prevent potential corruption, and identity information returns to the associated pool. Associated targets (for example, storage volume) are not affected.

NOTE: You cannot remove a chassis that is in a Pending state.

If you remove a server, the server state changes to Pending. The server powers off, ASM erases network identity information from the server to prevent potential corruption, and network identity information returns to the associated pool.

NOTE: Before you add new servers using existing iDRAC IP Address in an inventory, ensure that you remove the old servers from ASM before discovering the new servers.

Viewing the firmware and software compliance report

The following are the steps to view the firmware and software compliance report:

1. On the home page, click **Resources**.
2. Select a resource to view the compliance report.
3. In the right pane, click the link corresponding to **Firmware/Software Compliance**.
   The **Server Firmware/Software Compliance Report** page is displayed.
4. Click **Firmware Components** to view the firmware components.
5. Click **Software Components** to view the software components.

NOTE: To update the non-compliant resources, click Update Resources.

NOTE: If there is no catalog attached to the resource, you cannot perform the firmware update or software update.

Discovery overview

You can discover new resources or existing resources that are already configured within your environment. After discovery, you can deploy services on these resources from a template.

When ASM discovers a chassis, it also discovers servers and I/O modules within the chassis.

The **Discover Resources** wizard enables you to discover resources. To open the **Discover Resources** wizard, perform one of the following actions:

- On the **Getting Started** page, click **Discover Resources**.
- On the home page, click **Resources**. On the **Resources** page, click **Discover** in the **All Resources** tab.

Related links

Discovering resources

Discovering resources

NOTE: Only Administrator level users can discover resources.

Before you begin discovering the resources, gather the IP addresses and credentials associated with the resources, and ensure that:

- The resources are connected to the network.
- ASM virtual appliance is connected to the network.

NOTE: For some Dell resources such as chassis, servers, and I/O modules, the default credentials have been prepopulated in ASM. If the credentials have been changed from the defaults, add a new credential to ASM with the new login information.

To discover the resources:

1. On the **Welcome** page of the **Discover Resources** wizard, read the instructions, and click **Next**.
2. On the **Identify Resources** page, click **Add Resource Type**, and perform the following steps:
   a. Click **Resource Type**.
   b. From the **Resource** drop-down menu, select a resource that you want to discover.
   c. Type the Management IP address range of the resources that you want to discover in **IP Address Range*** field.

      NOTE: To discover a resource in an IP range, ensure that you provide the starting and ending IP addresses.

      NOTE: To discover the EMC storage, type the SP A IP Address and SP B IP Address in the IP Address Range field.

   d. Select one of the following options from the **Resource State** drop-down menu:

      - **Managed** — Select this option to monitor the firmware version compliance, upgrade firmware, and deploy services on the discovered resources. This is the default option.
      - **Unmanaged** — Select this option to monitor firmware version compliance only. The discovered resources are not available for a firmware upgrade or deploying services by ASM.
      - **Reserved** — Select this option to monitor firmware version compliance and upgrade firmware. The discovered resources are not available for deploying services by ASM.

   e. Select an existing or create a server pool from the **Discover into Server Pool** drop-down menu. This option allows you to discover the resources into the selected server pool instead of the global pool (default).

      NOTE: Selecting the server pool is optional.

   f. Select an existing or create a credential from the **Credentials** drop-down menu to discover resource types. The default options available are:

      - **Dell PowerEdge BMC Default** — Select PowerEdge servers with the BMC interface.

- **Dell PowerEdge iDRAC Default** — Select PowerEdge servers with the iDRAC interface.

3. Click **Next**.

   You may have to wait while ASM locates and displays all the resources that are connected to the managed networks.

   NOTE: To discover multiple resources with different IP address ranges, repeat step 2 and 3.

4. On the **Initial Chassis Configuration** page, perform the following tasks, and click **Next**.

   NOTE: The Initial Chassis Configuration page is displayed only when one or more chassis are identified in the specified IP range.

   NOTE: If you select both PowerEdge M1000e and FX2 chassis during Chassis configuration, the power configuration options for Enable Server Performance Over Power Redundancy or Enable Dynamic Power Supply Engagement are not displayed for selection. The two options are only applicable to PowerEdge M1000e chassis. It is recommended not to select both PowerEdge M1000e and PowerEdge FX2 chassis for chassis configuration.

   a. Under **Select Chassis For Initial Configuration**, select one or more chassis for which you want to assign IP address and add credentials during discovery.
   b. Under **IP Addressing** section, select the method for assigning IP address to chassis, servers, and I/O modules within the chassis.
   c. Under **Credentials** section, select credentials to access chassis, servers, and I/O modules within the chassis.

5. On the **Discovered Resources** page, select the resources from which you want to collect the inventory data, and click **Finish**.

   The discovered resources are listed in the **Resources** page.

Related links

Collecting the resource inventory
Adding IP Address and Credentials to Chassis

Adding IP Address and Credentials to Chassis

On the **Initial Chassis Configuration** page, you can configure the IP address and credentials to the chassis and the associated servers and I/O module during discovery. However, you can configure the global chassis settings and other unique settings for chassis, servers, and I/O modules using the Configure Resource wizard.

NOTE: The Chassis Configuration page in the Discover Resources wizard is displayed only when the resources that you discovered include one or more chassis.

1. On the **Initial Chassis Configuration** page, in the **IP Addressing** section, perform the following actions:

   a. Under Chassis, select one of the following methods for obtaining IP addresses for the chassis:

      - **Use existing chassis IP address** — ASM does not change the IP address of the chassis.

        NOTE: This option is valid only for chassis that have been previously configured and deployed inside or outside of ASM. Do not choose this option for new chassis.

        Assign static IP address from the network — Assign a static IP address from the pool of IP addresses in a management network. To add a network, click **New** and complete the **Define Network** page.

   b. Under Servers, select one of the following methods for obtaining IP addresses for the chassis:

      - **Use existing chassis IP address** — ASM does not change the IP address of the chassis.

        NOTE: This option is valid only for servers that have been previously configured and deployed inside or outside of ASM. Do not choose this option for new chassis.

      - **Assign IP address via DHCP** — Use DHCP to automatically allocate an IP address. This option is not valid for chassis.
      - **Assign static IP address from the network** — Assign a static IP address from the pool of IP addresses in a management network. To add a network, click **New** and complete the **Define Network** page.

c. Under I/O Modules, select one of the following methods for obtaining IP addresses for the chassis:

- **Use existing chassis IP address** — ASM does not change the IP address of the device.

  NOTE: This option is valid only for I/O modules that have been previously configured and deployed inside or outside of Active System Manager. Do not choose this option for new devices.

- **Assign IP address via DHCP** — Use DHCP to automatically allocate an IP address. This option is not valid for chassis.
- **Assign static IP address from the network** — Assign a static IP address from the pool of IP addresses in a management network. To add a network, click **New** and complete the **Define Network** page.

2. In the Credentials section, perform the following actions to select or modify the root credentials for chassis and associated servers and I/O modules:

   a. From the **Chassis Credentials** drop-down list, select the credentials for accessing the chassis. To create a root credential, click **Create New**. To edit a credential, select the credential from the **Chassis Credentials** drop-down list and click **Edit**.

   b. From the **Blade Credentials** drop-down list, select the credentials for accessing blade server within the chassis. To create a root credential, click **Create New**. To edit a credential, select the credential from the **Blade Credentials** drop-down list and click **Edit**.

   c. From the **I/O Module Credentials** drop-down list, select the credentials for accessing I/O modules within the chassis. To create a root credential, click **Create New**. To edit a credential, select the credential from the **I/O Module Credentials** drop-down list and click **Edit**.

3. Click **Next**.

Collecting the resource inventory

1. On the **Discovered Resources** page, select the resources from which you want to collect the inventory.
2. To collect the inventory data from the resources, click **Finish**.

   The discovered resources are listed in the **Resources** page.

Discovering an Enterprise Manager

Enterprise Manager is basically an element manager for Compellent storage. ASM may discover Compellent storage arrays as individual resources, but with the addition of Compellent iSCSI support, discovery of Enterprise Manager is also required.

To discover an enterprise manager, perform the following steps:

1. Go to **Settings** → **Credentials Management** → **Create**.
2. Select **Element Manager** from the **Credential type** drop-down menu.
3. Type the credential name and user name which you need to log in to the application.
4. Type the domain name in the **Domain Name** field which is an optional entry
5. Type the password and Confirm Password in the **Confirm Password** field.
6. Go to **Resources Discover** and click the **Discover** tab.
7. On the **Welcome** page of the **Discover Resources** wizard, read the instructions, and click **Next**.
8. On the **Identify Resources** page, click **Add Resource Type**, and perform the following steps:
   a. Select **Element Manger** from the **Resource Type** drop-down.
   b. Type the IP Address in the **Starting IP Address** field for the Element Manager.
   c. Select Element Manager from the **Element Manager** drop-down credentials.

      The Element Manager gets discovered.

      In the **Details** area on the right side, the run inventory details are not displayed as the support is provided in detail later.

Configuring resources or chassis

Use the **Configure Chassis** wizard to perform the following operations:

- Remove one or more resources from ASM environment. You can perform this operation only when you launch this wizard from **Getting Started** page.

- Enables you create your own custom firmware repository, import firmware repository from Dell Repository Manager (DRM), and perform firmware compliance check on the resources. You can perform this operation only when you launch this wizard from **Getting Started** page
- Enables you to on board or reconfigure one or more chassis and servers and I/O modules within the chassis.

NOTE:
When you configure the chassis and iDRAC users, the existing user account on the Chassis and iDRAC are erased and by the new user settings that is entered on the Chassis Configuration Wizard.

Before you begin, it is recommended to gather the following information:

- User names and passwords of accounts that can access the resources.
- Optionally, SMTP server and email address for an account to receive alerts.
- Optionally, NTP server IP addresses
- (Optional) Chassis Management Controller (CMC) and Integrated Dell Remote Access Controller (iDRAC) VLAN IDs.

1. On the **Welcome** screen, read the instructions, and click **Next**.
2. The **Discovered Resources** page lists the resources discovered in ASM. If you do not want one or more resources to be in ASM environment, select the resources, and click **Remove Resource from ASM**. Click **Next**.

   NOTE: The Discovered Resources, Default Firmware Repository, and Firmware Compliance pages are displayed only when you start this wizard from the Getting Started page.
3. On the **Default Firmware Repository** page, create and import your own custom repositories from DRM to use as the default firmware level for your discovered resources. Click **Next**.

   The **Firmware Compliance** page lists the resources that do not meet the firmware requirements specified by the default repository.
4. On the **Firmware Compliance** page, select the resources to update the firmware running on the resources automatically to meet the firmware requirements specified in the default repository. Click **Next**.
5. In the **Chassis Configuration** page, select one or more chassis to configure the following global settings, and then click **Next**. For more information, see Configure Global Chassis Configuration Settings.

   a. Under **Users**, configure more CMC and iDRAC local users.

   b. Under **Monitoring**, change the default monitoring settings.

   c. Under **NTP**, select the time zone and NTP servers.

   d. Under **Power Config**, configure power budget and redundancy attributes.

   e. Under **Networking**, add networking settings for the chassis.
6. On the **Unique Chassis Settings** page, configure specific chassis settings on chassis individually, and then click **Next**. For more information, see Configuring Unique Chassis Settings.
7. On the **Unique Server Settings** page, enter the iDRAC DNS name for the servers within the chassis, and then click **Next**. For more information, see Configuring Unique Server Settings.
8. On the **Unique IO Module Settings** page, enter a host name for each I/O module on chassis, and then click **Next**. For more information, see Configuring Unique I/O Module Settings.
9. On the **Uplink Port Configuration** page, configure uplink ports on the MXL switches within the chassis, and then click **Next**. For more information, see Configuring Uplink Ports
10. On the **Summary** page, verify the chassis configuration settings and click **Finish** to configure the chassis.

Related links

Removing discovered resources
Configuring default firmware repository
Running firmware compliance
Configuring global chassis settings
Configuring unique chassis settings
Configuring unique I/O module settings
I/O module configuration
Completing the chassis configuration

Removing discovered resources

The **Discovered Resources** page list the resources discovered in ASM.
On this page, you can select one or more resources that you do not want to be in ASM environment, and click **Remove**.

When you are performing next configuration steps using Configure Resource dialog, ASM enables you to:

- Create a default firmware repository
- Perform a firmware compliance check on these resources against the firmware level specified in the default repository.
- Allows you to update the firmware as needed.
- Configure one or all chassis that have been discovered.

Configuring default firmware repository

On the Default Firmware Repository page, you can:

- Click **Add Repository** to create firmware repositories.
- Click **Remove** to remove a repository
- Click **View Details** to view the firmware bundles that are available in the firmware repository.
- To set the repository as default firmware repository, select a repository from the list and click **Set as Default**.

Running firmware compliance

ASM requires a minimum firmware level for all resources it manages.
The **Firmware Compliance** page list the resources that do not meet the firmware requirements specified in the default repository that you have set in the previous step.

On this page, select the resources that you want to update the firmware automatically, click **Next**.

If you skip the automatic firmware update, in the **Resources** → tab, the **Firmware Compliance** state of the resources that is not compliant is displayed as either **Update Required** or **Non-Compliant**.

NOTE: When updating firmware, you may see logs indicating a firmware failure. These logs can be ignored if the devices are in a compliant state when the chassis configure job is complete.

Configuring global chassis settings

1. On the **Chassis Configuration** page of the Configure Chassis wizard, select one or more chassis that you want to configure.
2. Under Select Chassis for Initial Configuration, select one or more chassis that you want to configure.
3. Under **Global Settings**, in the **Users** section, configure more CMC and iDRAC local users.

    a. To add new Chassis Management Controller (CMC) user, under CMC Users, click **Create**. For more information, see Adding or Editing a Chassis Management Controller (CMC) User.

To edit a user account, select a CMC user from the list, and click **Edit**. To delete a user account, select the user accounts from the list, and click **Delete**.

b. To add new Integrated Dell Remote Access Controller (iDRAC) user, under iDRAC Users, click **Create**. For more information, see Adding Or Editing An Integrated Dell Remote Access Controller (iDRAC) User.

4. Under **Global Settings**, in the **Monitoring** section, configure the following settings:

a. To set SNMP trap alert destination, perform the following steps:

1. Under **Alert Destinations**, to add an SNMP trap alert destination for chassis, click **Create**.

   To edit Alert Destinations, select an alert destination from the list, and click **Edit**. To delete an alert destination, select an alert destination from the list, and click **Delete**.

2. Enter a valid **Destination IP Address**. Use the quad-dot IPv4 format (for example, 10.10.10.10) or Fully Qualified Domain Name (for example, dell.com).

3. Enter the **Community String** to which the destination management station belongs.

b. In the **Email Alert Settings** section, to configure the CMC to send email alerts to one or more email addresses:

1. In the **SMTP Server** box, enter the IP address or host name of an SMTP Server that receives email alerts.

2. Click **Create** and enter the following:

   - In the **Name** box, enter the source email name from which the email alerts are sent.
   - Enter one or more **Destination Email Addresses**.

c. In the **Syslog Configuration (for I/O Modules only)** section, enter the **Syslog Destination IP Address** to send I/O module log messages to a Syslog Destination.

5. Under **Global Settings**, in the **NTP** section:

a. Enter the **Time Zone** in which the chassis is located.

b. To synchronize the chassis clock with an NTP server, select **Enable NTP Server** check box and enter the host names or IP addresses of the **Primary NTP Server** and **Secondary NTP Server** (Optional).

6. Under **Global Settings**, in the **Power Config** section:

a. From the **Redundancy Policy** drop-down list, select one of the power redundancy policies that you want to configure on the chassis:

   - **No Redundancy** — The chassis is not configured with power redundancy.
   - **Power Supply Redundancy** — A PSU in the chassis is kept as a spare, ensuring that the failure of any one PSU does not cause the servers or chassis to power down.
   - **Grid Redundancy** — This policy divides the available PSUs into two power grids. PSU 1 is power grid 1 and PSU 2 is power grid 2. For maximum power, the PSUs should have the same capacity. If a grid or PSU fails, then the power is provided by the remaining PSU.

b. Optionally, select **Server Performance Over Power Redundancy** check box to favor server performance and power up over maintaining power redundancy.

c. Optionally, select **Enable Dynamic Power Supply Engagement** check box to allow the chassis controller to put underutilized PSUs into standby mode based on the redundancy policy and system power requirements.

7. Under **Global Settings**, in the **Networking** section:

a. Optionally, select **Register Chassis Controller on DNS** check box to enable users to access the Chassis Management Controller (CMC) with a user-friendly name, instead of an IP address.

b. Optionally, select **Register iDRAC on DNS** check box to enable users to access the Integrated Dell Remote Access Controller (iDRAC) with a user-friendly name, instead of an IP address.

c. Optionally, select **Enable IPMI over LAN** check box to enable or disable the IPMI over LAN channel for each iDRAC present in the chassis.

8. To configure the unique chassis settings, click **Next**.

Related links

Adding or editing Chassis Management Controller (CMC) user

Adding or editing Integrated Dell Remote Access Controller (iDRAC) user

Configuring unique chassis settings

1. On the **Unique Chassis Settings** page of the Configure Chassis wizard, to modify the settings that are specific for each individual chassis, select the **Configure Unique Chassis Settings** check box.

   The **Unique Chassis Settings** page lists the chassis that you want to configure.

2. To configure a chassis, click the arrow left to the chassis title, and enter the following information:
   - **Chassis Name** — Enter the name identify the chassis.
   - **CMC DNS Name** — Enter DNS name of the chassis.
   - **FD332 Storage Node** — For FX2 chassis, depending on your configuration, select one of the following options from the **FD332 Storage Node** drop-down menu:
     - **Split Single Host**
     - **Split Dual Host**
     - **Joined**

     For FX2 chassis with FC430, select **Split Dual Host**.

     For FX2 chassis with FC630, select **Split Single Host**.
   - **System Input Power Cap** — Enter the maximum power limit that can be input to the system. You can specify the maximum power limit in one of the following units:
     - **Watts** — Automatically calculated during runtime.
     - **BTU/h** — British Thermal Unit. For example, 16719.
     - **%** — Type a value that indicates the actual percentage of power input versus the maximum power that can be supplied.

3. Optionally, click **Enter Location Details**, and enter the following information:
   - **Datacenter** — Indicates the name of the data center.
   - **Aisle** — Indicates the name of the aisle.
   - **Rack** — Indicates the name of the rack server.
   - **Rack Slot** — Indicates the bottom rack slot of the chassis when it is mounted in the rack server.

Configuring unique server settings

1. On the **Unique Server Settings** page of the Configure Chassis wizard, to modify the settings for the servers within the chassis, select **Configure Unique Server Settings** check box.

   The **Unique Server Settings** page lists the servers within the chassis that you have selected. Each section in this page represents a chassis and servers within that chassis. Click the arrow next to the section title to expand or collapse the section.

   The following information is displayed for each server:
   - **Service Tag** — Displays the service tag for the server. The service tag is a unique identifier provided by the manufacturer for support and maintenance. If the server is absent, this field is empty.
   - **Slot** — Identifies the server location.
   - **Management IP** — Displays the management IP address of the server.

2. If you want to modify the iDRAC DNS Name of the server, in the **iDRAC DNS Name** column, enter an iDRAC DNS name for the server.

3. To configure the IO modules within the chassis, click **Next**.

Configuring unique I/O module settings

1. On the **Unique I/O Module Settings** page, select **Configure Unique I/O Module Settings** check box to modify the unique settings for the IO modules with in the chassis.

   The **Unique I/O Module Settings** page lists the I/O modules within the chassis that you have selected. Each section in this page lists the I/O modules within a chassis. Click the arrow left to the section to expand or collapse the section.

   The page displays the following information about the I/O modules that have been discovered:

   - **Service Tag** — Displays the service tag of the I/O module. The service tag is a unique identifier provided by the manufacturer for support and maintenance.
   - **Fabric Slot** — Indicates the slot name where the I/O module is present.
   - **Management IP** — Displays the management IP address of the server.
   - **Host Name** — Displays the host name of the I/O module.
2. If you want to modify the host name of the I/O module, in the **Host Name** column, enter the host name for the corresponding I/O modules.
3. To configure the uplink ports, click **Finish**.

I/O module configuration

Use this page to configure uplinks on the MXL Switches and IOAs within one or more chassis.

NOTE: ASM supports configuration of uplinks on MXL Switches and IOAs. It supports VLT workload network configuration too.

NOTE: MXL is a 10Gb/40Gb Ethernet blade switch used in our M1000E chassis. During the ASM onboarding process we can configure management IP address, credentials, basic management settings, and configure an uplink to the top of rack networking device for the chassis.

An I/O module is a switch for a blade chassis.

From this page, you can:

- Define the uplinks. For more information, see Defining Uplinks.
- Upload switch configuration file. For more information, see Upload Switch Configuration File
- Enable VLT. For more information, see VLT Enabled
- Configure the uplinks in one of the following ways:
  - Configure the same ports as uplink ports in all the chassis. See Configure the uplink ports differently in all the chassis
  - Configure the uplink ports differently in all the chassis. See ConfigureChassis: Configuring Uplink Ports on Each I/O Module Independently

Related links

Defining uplinks
Configuring The uplinks on Each I/O Module Independently
Configuring uplink ports on all chassis independently

Defining uplinks

1. On the **Uplink Port Configuration** page of the Configure Chassis wizard, in the Configure Uplinks area, click **Define Uplinks**.
2. In the **Define Uplinks** dialog box, click **Add Uplink**, and enter the following:

   a. Enter the name for the uplink.

   b. From the Port Channel drop-down list, select the port channel that you want to create on the switch.

c. From the Network Type drop-down list, select one or more networks that you want to assign to the uplink.

The **Network Name(s)** column displays the networks that are assigned to the uplinks.

To delete an uplink, click the **Delete** icon left to the corresponding uplinks.

3. Repeat step 2 to define multiple uplinks.
4. Click **Save**.

After you define and save uplink, uplink is available to get applied to switch.

Upload Switch Configuration File

This feature is supported for MXL in M1000e Chassis only.
By using this feature, you can upload a preconfigured switch configuration file instead of configuring through the I/O Module Configuration.

To upload switch configuration file:

1. Select **Upload Switch Configuration File** option. After you select the option, **File Name**, **File Description field**, **Upload File** field tab are appeared.

   Enter the result of your step here (optional).
2. Type the file name which you want to upload in **File name** field.
3. Type a file description which about the file in **File Description** field.
4. Click **Browse** beside **Upload File** tab. It directs you to your local system where you have saved the file.
5. Select the file and click **Open** to upload it.

NOTE: After you upload the switch configuration file, it gets uploaded on switch. It takes existing IPs from the switch and pulls it out and upload to the configuration file. It gets applied on all selected switches what you have chosen to configure. It also pulls out the host name and credentials.

Configuring uplink ports on all chassis independently

1. On the **I/O Module Configuration** page, select the **Configure Uplinks** check box.
2. Select **Configure Uplink Ports on All Chassis independently** option.

   Select the arrow left to the section title to expand the section.
3. Select any one of the following options from the **Spanning Tree Mode** drop-down menu:
   - **RSTP** (Rapid Spanning Tree Protocol)
   - **MSTP** (Multiple Spanning Tree Protocol)
   - **PVST** (Per VLAN Spanning Tree Protocol)
   - **None**

NOTE: The Spanning Tree Mode option is applicable only for Dell networking MXL switches in Dell PowerEdge M1000e.

4. In the Configure Uplinks area, expand the chassis section, and perform one of the following actions:
   - Select the **Configure uplinks on each I/O Module Independently** check box to configure different ports as uplink ports in each I/O module.

     The table lists ports that are available in each I/O module in separate columns.
   - Clear the **Configure the uplinks on each I/O Module Independently** check box to configure the same ports as uplink ports across all I/O modules.

     The table displays the following information:
     - IO modules (Model Name) that is present in each fabric.
     - Ports that are available in each IO module.
5. In the table, select the **Quadport mode** check box if you want to run the port in Quad mode.

When a 40 GbE port is run in quad mode, it provides four 10 GB Ethernet interfaces that number sequentially starting with the port number of the 40GbE interface. For example, when **Quadport mode** is enabled on the GbE port number 33, it makes four 10GbE links with the port numbers 33, 34, 35, and 36.

6. From the drop-down list next to the corresponding port numbers, select the uplink that you want to configure on each port.

   NOTE: Uplink is an interconnect (also called port-channel, or grouping of ports) which is created on a switch by creating a connection to other switches in a networking environment. ASM can configure uplinks on MXLs, I/O Aggregators, FN410S, and FN2210S switches (I/O modules).

7. Click **Next** to configure uplink port on all chassis independently.

   NOTE: Uplink is an external connection from chassis switch to customer network environment. Customer is still required to configure corresponding ports and uplinks on the top of rack switches, ASM only configures the chassis.

Configuring The uplinks on Each I/O Module Independently

1. On the **I/ O Module Configuration** page, select the **Configure Uplinks** check box.
2. Select **Configuring The uplinks on Each I/O Module Independently** option.
3. In the Configure Uplinks area, perform one of the following actions:
   - Select the **Configure the uplinks on each I/O Module Independently** check box to configure different ports as uplink ports in each I/O module.

     The table lists ports that are available in each I/O module in separate columns.
   - Clear the **Configure the uplinks on each I/O Module Independently** check box to configure the same ports as uplink ports across all I/O modules.

     The table displays the following information:
     - IO modules (Model Name) that is present in each fabric.
     - Ports that are available in each IO module.
4. In the table, select the **Quadport Mode** check box if you want to run the port in Quad mode.

   When a 40 GbE port is run in quad mode, it provides four 10 GB Ethernet interfaces that number sequentially starting with the port number of the 40GbE interface. For example, when **Quadport mode** is enabled on the GbE port number 33, it makes four 10GbE links with the port numbers 33, 34, 35, and 36.
5. From the drop-down list next to the corresponding port numbers, select the Uplink that you want to configure on each port.

   NOTE: Uplink is an interconnect (also called port-channel, or grouping of ports) which is created on a switch by creating a connection to other switches in a networking environment. ASM can configure uplinks on MXLs, I/O Aggregators, FN410S, and FN2210S switches (I/O modules).

6. Click **Next**.

   NOTE: Uplink is an external connection from chassis switch to customer network environment. Customer is still required to configure corresponding ports and uplinks on the top of rack switches, ASM only configures the chassis.

VLT Enabled

VLT is a layer-2 Link Aggregation Group for a server, switch, or any device that supports LACP to two different upstream devices. This can be used between two peer switches, for example in a chassis.

VLT is enabled to create redundant, load-balancing connections to different switches or to servers. If one switch fails or goes down for maintenance, the other switch can be used to pass traffic until the other switch is brought back online.

If you enable VLT, you can select VLT from port drop-down menu. Same should be selected in corresponding port, so that it can correspondent port to port.

If you enable VLT, you can select VLT from the port drop-down menu. The same should be selected in the corresponding port on the other switch, so that it can correspond port to port. It is not mandatory to have VLT enabled.

NOTE: On PowerEdge M1000e systems, you can select either VLT or Uplink for any of the ports, however, you must ensure to match port-to-port.

NOTE: VLT configuration does not support using both 10 Gb and 40 Gb ports at the same time. Ensure that you use the same type of port while configuring VLT.

Completing the chassis configuration

1. On the **Summary** page, click **Finish** to apply the configuration on the chassis you have selected.
   In the **Resources** → **All Resources** tab, the state of the chassis is displayed as **Updating** until the configuration is complete.
2. If you want to modify the chassis configuration settings, click **Back**.

Adding or editing Chassis Management Controller (CMC) user

1. On the **Create Local User** page, enter **User Name** of an account.
2. Enter the **Password** for the user account to log in to CMC. Reenter the password for confirmation.
3. Select one of the following **Roles** to assign to user account:
   - **Administrator**
   - **Power User**
   - **Guest User**
   - **None**
4. To enable this user account, select **Enable User** check box. Clear the Enable User check box to add the user in a disabled state.

Adding or editing Integrated Dell Remote Access Controller (iDRAC) user

1. On the **Create Local User** page, enter **User Name** of an account.
2. Enter the **Password** for the user account to log in to iDRAC. Reenter the password for confirmation.
3. Select one of the following **Role** to assign to user account:
   - **User**
   - **Operator**
   - **Administrator**
   - **No Access**
4. To enable this user account, select **Enable User** check box. Clear the **Enable User** check box to add the user in a disabled state.

Updating resource inventory

NOTE: Only the user with Administrator or Standard role can run the inventory on the resources. However, Standard user can only run the inventory on the resources that are part of server pool for which they have permission.

To manually run the inventory operation and update ASM with the latest resource data:

1. On the home page, click **Resources**.
2. On the **Resources** page, click the **All Resources** tab.
3. From the list of resources, click a resource, and in the **Details** pane, click **Run Inventory**.
   When you select C- series server on resource page and click **Run inventory**, you will not get all the inventory details for C 622O server. You will only get basic information about it. After you deploy the server, you will get detailed information about it.

   An inventory job is scheduled, the resource state changes to Pending. When the inventory is complete, the resource state changes to Available. See ASM logs to view the start time and end time of the resource inventory operation.

Viewing resource details

NOTE: Standard users can only view the details of resources that are part of server pools they have permissions on.

To view the details about a resource, perform the following steps:

1. On the home page, click **Resources**.
2. In the **Resources** page, select the **All Resources** tab.
3. From the list of resources, select a resource for which you want to view the details.
4. Click **View Details** in the right pane.

From this **View Details** pane, you can:

- View detailed information about the resources and associated components.

  NOTE: In ASM 8.3 release, the detailed information can be viewed only for Dell Resources.

- Update resource inventory data.

NOTE: After discovery of a C6220 server, you will not have detailed information regarding network interfaces or firmware versions. You will get more detailed information after you deploy the server.

For 13 G servers, you get performance details along with resource details.

Performance details include:

- System Usage
- CPU Usage
- Memory Usage
- I/O Usage

NOTE: These performance usage values get updated every five minutes.

Historical data and peak value information are available under each Chronograph of Usage information.

If you click **Historical Data**, a drop-down menu appears. You can select **Last Week**, **Last Month**, **Last Year** from the **Historical Data** drop-down menu. You get average, minimum, maximum value according to your selection.

If you click **Peak Values**, you get information regarding peak value, peak time, and start time.

Related links

Viewing chassis details
Viewing blade or rack server details
Viewing storage group details
Viewing VMware vCenter details

Viewing chassis details

1. On the home page, click **Resources**.
   The **Resources** page is displayed.
2. In the **All Resources** tab, click a chassis from the list of resources to view the details.
   The **Details** pane in the right displays the basic information about the Chassis, such as Power State, Management IP, Chassis Name, Service Tag, and Location.
3. To view the detailed information about the Chassis, in the **Details** pane, click **View Details**.
   The **Chassis Details** page displays the detailed information about the Chassis in the following tabs.

   NOTE: In the current release, the detailed information can be viewed only for Dell Chassis.

- **Summary**
- **Port View**
- **Blades**
- **I/O Modules**
- **Chassis Controllers**
- **IKVM**
- **Power Supplies**

From the **Summary** tab of the **Chassis Details** page, you can:

- Open the remote GUI console for a Chassis Management Controller (CMC).
- View all recent activities performed on the Chassis.

Viewing blade or rack server details

1. On the home page, click **Resources**.
   The **Resources** page is displayed.
2. In the **All Resources** tab, click a blade server or rack server from the resources list to view the details.
   The **Details** pane on the right displays basic information about VMware vCenter, such as Power State, Management IP, Datacenters, Clusters, Hosts, and Virtual Machines.
3. In the **Details** pane, click **View Details**.
   The **Blade Server Details** page displays the detailed information about the server in the following tabs.

   NOTE: In the current release, the detailed information can be viewed only for Dell Servers.

   - **Summary**
   - **Port View**
   - **Network Interfaces**
   - **Firmware Revisions**
   - **CPUs**
   - **Memory**

From the **Blade Server Details** page, you can:

- Open the remote console of the server's Integrated Dell Remote Access Controller (iDRAC).
- View recent activities performed on the server.

Viewing VMware vCenter details

1. On the home page, click **Resources**.
   The **Resources** page is displayed.
2. In the **All Resources** tab, click VMware vCenter from the resource list to view the details.
   In the right pane, you can see the basic information about the VMware vCenter, such as Power State, Management IP, Data centers, Clusters, Hosts, and Virtual Machines
3. Also, in the **Details** pane, under **vCenter Details**, click the arrows to expand **vCenter** → **Datacenter** → **Cluster** to view the lists of nodes and applications.

Viewing SCVMM details

1. On the home page, click **Resources**.
   The **Resources** page is displayed.
2. In the **All Resources** tab, click a System Center Virtual Machine Manager (SCVMM) from the resource list to view the details.
   The **Details** pane in the right displays the following basic information about the SCVMM:

- Health
- Management IP
- Host Groups
- Clusters
- Hosts
- Virtual Machines

3. Also, in the **Details** pane, under **SCVMM Details**, click the arrows to expand **SCVMM** → **Host Groups** → **Hosts** → **Clusters** to view the lists virtual machines, nodes, and applications.

Viewing storage group details

1. On the home page, click **Resources**.
   The **Resources** page is displayed.
2. In the **All Resources** tab, click a storage group from the resources list to view the details.
   In the right pane, you can see the basic information about the storage group, such as System Status, Management IP, Storage Center Name, Group Members, Volumes, Replay Profile, Free Group Space. For NetApp storage type, displays the Storage Name, Available Storage, Aggregates, Volumes, and Disks.
3. In the **Details** pane, click **View Details**.
   The **Storage Group** details page displays detailed information about storage group in the following tabs:
   - Summary
   - Volumes

   NOTE: In ASM 8.3 release, the detailed information can be viewed only for Dell Resources.

From the **Storage Group Details** page, you can view the recent alerts about the storage, and additionally:

- For Dell EqualLogic Storage, you can open the element manager GUI of Group Manager.
- For Dell Compellent Storage, you can open the element manager GUI of Storage Center.

Viewing storage details

The following are the steps to view the storage details:

1. On the home page, click **Resources**.
   The **Resources** page is displayed.
2. In the **All Resources** tab, from the **Resource Type** drop-down menu, select **Storage**.
   The list of storage array is displayed.
3. Select a storage array to view the details.
   In the right pane, the following information about the storage is displayed:
   - **In Use in Service(s)**
   - **Firmware/Software Compliance**
   - **Resource Name**
   - **Health**
   - **Management IP**
   - **LUNs**
   - **Free Disk Space**
   - **SP A IP Address**(only for EMC storage)
   - **SP B IP Address** (only for EMC storage)
4. In the right pane, click **View Details**.
   The **Storage Details** page displays the detailed information about the server in the following tabs:

- **Summary**
- **LUNs**
- **Volumes**

Opening the iDRAC remote console

To simplify routine server maintenance, you can open a remote console to the server's Integrated Dell Remote Access Controller (iDRAC) directly from ASM:

NOTE: For more information, see the *Integrated Dell Remote Access Controller User Guide*.

1. On the home page, click **Resources**.
2. On the **Resources** page, click the **All Resources** tab.
3. Click a server.
4. In the **Details** pane, click **View Details**.
5. In the **Summary** tab, under **Actions**, click **Launch iDRAC GUI**.

Opening the CMC remote console

To simplify routine Chassis maintenance, you can open a remote console to the server's Integrated Chassis Management Controller (CMC) directly from ASM:

NOTE: For more information, see the *Chassis Management Controller User Guide*.

1. In the left pane, click **Resources**.
2. On the **Resources** page, click **All Resources** tab.
3. Click a Chassis from the list.
4. In the **Details** pane, click **View Details**.
5. In the **Summary** tab, under **Actions**, click **Launch CMC GUI**.

Understanding server pools

In ASM, a Server Pool is a set of servers grouped for specific use-cases such as business units or workload purposes. An administrator can also specify a set of users who can access these server pools.

The **Server Pools** tab lists the existing server pools and enables you to perform the following actions:

NOTE: Standard users can view only the details of the server pools for which they have permissions.

NOTE: A user with Administrator role can only create, edit or delete the server pools.

- Create or edit server pools
- Delete existing server pools

Click a server pool from the list to view detailed information in the following tabs:

- **Servers** — Lists the number of servers associated with the server pool.
- **Users** — Lists the number of users who has the access rights to the server pool.

Related links

Creating server pool
Application logs
Users
Repositories
About roles
Jobs
Virtual appliance management

Creating server pool

1. On the home page, click **Resources**, and then click **Server Pools**.
2. In the **Server Pools** tab, click **Create New**.
   The **Create Server Pool** wizard is displayed.
3. On the **Welcome** page, read the instructions, and click **Next**.
4. On the **Server Pool Information** page, type the name and description for the server pool. Click **Next**.
5. On the **Add Servers** page, select the servers that you want to add to the server pool. Click **Next**.
6. On the **Assign Users** page, select the users you want to grant access rights to the server pool. Click **Next**.
7. On the **Summary** page, review the server pool configuration, and then click **Finish**.

Editing server pool

1. On the home page, click **Resources**, and then click **Server Pools**.
2. In the **Server Pools** tab, click **Edit**.
   The **Create Server Pool** wizard is displayed.
3. To change the name and description of the server pool, in the left pane, click **Server Pool Information**. Click **Save**.
4. To add or remove servers from the server pool, in the left pane, click **Add Servers**. Click **Save**.
5. To add or remove the access rights to the server pool, in the left pane, click **Assign Users**. Click **Save**.

Deleting server pool

1. In the **Server Pools** tab, select one or more server pools, and click **Delete**.
2. Click **OK** when the confirmation message is displayed.

8

Settings

On the **Settings** page, you can:

NOTE: A user with Administrator role can only configure the following settings. For more information about roles and permission, see About Roles

- Create Add-on module.
- Configure automatically scheduled and manual backup and restore jobs.
- Create the credentials that ASM use to access chassis, server, switch, VMware vCenter, and storage resources.
- Access the Getting Started page.
- Access application logs.
- Manage OS image and firmware repositories.
- View and cancel Jobs.
- Define existing networks.
- Manage ASM users.
- Perform appliance management tasks related to NTP settings, proxy server settings, SSL certificates, and license management for the ASM virtual appliance.
- Create virtual identity pools.

Related links

Networks
Credentials management
Virtual identity pools
Backup and restore

Add-On Modules

Add-On Modules are zip files that can be uploaded to the Application section for Templates in ASM. These files contain the description for the applications.

Related links

Creating an Add-On Module

Creating an Add-On Module

1. Click **Settings**.
2. On the left pane, click **Add-On Modules**.
3. Click **+Add**.
   The Add Module window is displayed.
4. Click **Browse**.
5. Select the module zip file to upload and click **Open**.
6. Click **Save**.
   The file is displayed on the Add-On Modules page and the contents of the file are copied to the location in the ASM appliance.

NOTE: An error message is displayed if you try adding an existing module.

To remove an existing Add-On module, click the delete icon beside the module that you want to delete.

Backup and restore

Performing a backup saves all user-created data to a remote share from which it can be restored.

NOTE: It is recommended to perform frequent backups to guard against data loss and corruption. Also, it is recommended to take a snapshot of ASM virtual appliance every time you perform a restore (for more information, see VMware documentation).

The **Backup and Restore** page displays information about the last backup operation performed on ASM virtual appliance. Information in the **Settings and Details** section applies to both manual and automatically scheduled backups and includes the following:

- Last backup date
- Last backup status
- Backup directory path to an NFS or a CIFS share, including an optional user name required to access the share, if necessary
- Backup Directory User Name

Also, the **Backup and Restore** page displays information about the status of automatically scheduled backups (Enabled or Disabled).

On this page, you can:

- Manually start an immediate backup
- Restore earlier configuration
- Edit general backup settings
- Edit automatically scheduled backup settings

Related links

Backup now
Restore now
Editing backup settings and details
Editing automatically scheduled backups

Backup details

ASM backup file includes following information:

- Activity logs
- Credentials
- Deployments
- Resource inventory and status
- Events
- Identity Pools
- Initial setup
- IP addresses
- Jobs
- Licensing
- Networks
- Templates
- Users and roles

- Resource Module configuration files

Editing backup settings and details

1. On the home page, click **Settings**, and then click **Backup and Restore**.
2. On the **Backup and Restore** page, under **Settings and Details** section, click **Edit**.

   The **Settings And Details page** is displayed.
3. Optionally, to indicate the network share location where the backup file is saved, type a backup directory path in the **Backup Directory Path** box. Use one of the following formats:
   - NFS — host:/share/
   - CIFS — \\host\share\

   If username and password are required to access the network share, in the **Backup Directory User Name** and **Backup Directory Password** boxes, you can type a user name and a password.
4. To open the backup file, in the **Encryption Password** box type a password. Verify the encryption password by typing the password in the **Confirm Encryption Password** box.

   NOTE: The password can include any alphanumeric characters such as!@#$%*
5. Click **Save.**

Editing automatically scheduled backups

On this page, you can specify the days and time to run automatically scheduled backups. To change the location where backup files are saved or the password accessing a backup file, see Editing Backup Settings and Details.

1. On the home page, click **Settings**, and then click **Backup and Restore**.
2. On the **Backup and Restore** page, under the **Automatically Scheduled Backups** section, click **Edit**.

   The **Automatically Scheduled Backup** dialog box is displayed.
3. To schedule automatic backups, next to **Automatically Scheduled Backups**, select **Enabled**. To discontinue automatically scheduled backups, select **Disabled.**
4. To specify day(s) on which backup must occur, select the days in **Days for Backup**.
5. From the **Time for Backup** drop-down list, select the time.
6. Click **Save**.

Backup now

In addition to automatically scheduled backups, you can manually run an immediate backup.

1. On the home page, click **Settings**, and then click **Backup and Restore**.
2. On the **Backup and Restore** page, click **Backup Now**.
3. Select one of the following options:
   - To use the general settings that are applied to all backup files, select **Use Backup Directory Path and Encryption Password from Settings and Details**.
   - To use custom settings:

     1. In the **Backup Directory Path** box, type a path name where the backup file is saved. Use one of these formats:

        – NFS — host:/share/

        – CIFS — \\host\share\
     2. Optionally, type a username and password in the **Backup Directory User Name** and **Backup Directory Password** boxes, if they are required to access the location you typed in the earlier task.
     3. In the **Encryption Password** box, type a password that is required to open the backup file, and verify the encryption password by typing the password in the **Confirm Encryption Password** box.

NOTE: The password can include any alphanumeric characters such as!@#$%*

4. Click **Backup Now**.

Restore now

Restoring ASM virtual appliance returns user-created data to an earlier configuration that is saved in a backup file.

CAUTION: Restoring an earlier configuration restarts ASM virtual appliance and deletes data created after the backup file to which you are restoring.

NOTE: It is recommended to perform frequent backups to prevent data loss and corruption. Also, it is recommended to take a snapshot of ASM virtual appliance every time you perform a restore (for more information, see VMware documentation).

1. On the home page, click **Settings**, and then click **Backup and Restore**.
2. On the **Backup and Restore** page, click **Restore Now**.
3. Type a path name in the **Backup Directory Path and File Name** box that specifies the backup file to be restored. Use one of the following formats:
   - NFS — host:/share/filename.gz
   - CIFS — \\host\share\filename.gz
4. To log in to the location where the backup file is stored, type the username and password in the **Backup Directory User Name** and **Backup Directory Password** boxes.
5. To access the backup file, type the encryption password in the **Encryption Password** box. This is the password that was typed when the backup file was created.
6. Click **Restore Now**.
7. Confirm or cancel the action when a confirmation message is displayed.

The restore process is started.

Credentials management

ASM requires a root-level user name and password to access and manage chassis, servers, switch, VMware vCenter, and storage.

NOTE: To access any Dell resource, the default root-level user name is *root*, and the default password is *calvin*. It is recommended to change the password; however, the user name for root-level credentials in ASM must remain *root*.

NOTE: The Dell default credentials are not available for Dell Compellent Storage Center and Dell EqualLogic Storage. You must create credentials to access these Dell resources. To create credentials for the storage resource types, in the left pane, click Settings, and then click Credential Management.

The **Credentials Management** page displays the following information about the credentials:

- **Name** — User-defined name that identifies the credentials.
- **Type** — Type of resource that uses the credential.
- **Resources** — Total number of resources to which the credential is assigned.

From the credential list, click a credential to view its details in the **Summary** tab:

- Name of the user who created and modified the credential.
- Date and time that the credential was created and last modified.

On the **Credentials Management** page, you can:

- Create New Credentials
- Edit Existing Credentials

- Delete Existing Credentials

Related links

Creating credentials
Editing credentials

Creating credentials

To create credentials:

1. On the home page, click **Settings**, and then click **Credentials Management**.
2. On the **Credentials Management** page, click **Create**.
3. In the **Create Credentials** dialog box, from the **Credential Type** drop-down list, select one of the following resource types for which you want to create the credentials:
   - **Chassis**
   - **Server**
   - **Switch**
   - **vCenter**
   - **SCVMM**
   - **Storage**
   - **Element Manager**
4. In the **Credential Name** field, type the name to identify the credential.
5. In the **User Name** field, type the user name for the credential.

   NOTE: *root* is the only valid user name for root-level credentials on chassis (CMC), servers (iDRAC), and I/O modules. You can add local CMC and iDRAC users with user names other than *root*.
6. In the **Password** and the **Confirm Password** boxes, type the password for the credential.

   NOTE: For valid user name and password formats, see the iDRAC, CMC, I/O module, or see the storage third-party documentation.
7. Optionally, for VMware vCenter, SCVMM and **Element Manager**, in the **Domain** box, enter the domain ID.
8. Optionally, for switch credentials:
   a. Under **Protocol**, click one of the following connection protocols used to access the resource from remote.
      - **Telnet**
      - **SSH**
   b. Under **SNMP Configuration**, in the **SNMP v2 Community String** box, type the SNMP v2 community string required to access the resource.
9. To save the credential, click **Save**.

Related links

Editing credentials
Deleting credentials

Editing credentials

To edit a credential:

1. On the home page, click **Settings**, and then click **Credentials Management**.
2. On the **Credential Management** page, click a credential that you want to edit, and then click **Edit**.
3. Modify the credential information in the **Edit Credentials** dialog box.
4. Click **Save**.

Deleting credentials

To delete a credential:

1. On the home page, click **Settings**, and then click **Credentials Management**.
2. On the **Credential Management** page, select the credential that you want to delete, and then click **Delete**.
3. Click **OK** when the confirmation message is displayed.

Getting Started

This page provides a recommended guided workflow for getting started with ASM. A check mark indicates that you have completed the step.

Application logs

ASM provides an activity log of user- and system-generated actions to use for troubleshooting activities. By default, log entries display in the order they occurred.

You can view the following information:

- Severity
  -  — Indicates that the fatal error occurred while communicating with a managed resource; corrective action is immediately required.
  -  — Indicates that the resource is in a state that requires corrective action, but does not impact overall system health. For example, a discovered resource is not supported.
  -  — Indicates general information about system health or activity.
  -  — Indicates that the component is working as expected.
- Category
  - Security — Indicates the authentication failures, operations on ASM users, operations on credentials
  - Appliance Configuration — Indicates the initial setup, appliance settings, backup and restore
  - Template Configuration — Indicates the operations on Service Templates
  - Network Configuration — Indicates the operations on networks, pools for MAC/IQN/WWPN/WWNN
  - Infrastructure or Hardware Configuration — Indicates the hardware discovery, inventory
  - Infrastructure or Hardware Monitoring — Indicates the hardware health
  - Deployment — Indicates the Service template deployment operations
  - Licensing — Indicates the license updates and expirations
  - Miscellaneous — Indicates all other issues
- Description — Displays brief summary of activity
- Date and Time — Indicates the time when activity occurred and time is displayed using the client machine time zone. If there are logs, the time captured when the message is logged is based on the appliance time.
- User — Indicates user name from which activity originated

On this page, you can:

- View log entries
- Export all log entries to a **.csv** file
- Purge all log entries

NOTE: To sort entries by a specific category, click the arrow next to a column name.

Exporting all log entries

You can export all current log entries to a comma-delimited (**.csv**) file for troubleshooting.

1. On the home page, click **Settings**, and then click **Application Logs**.
2. On the **Application Logs** page, click **Export All**.
3. Open or save the file.

Purging log entries

You can delete log entries based on date and severity.

1. On the home page, click **Settings** and then click **Application Logs**.
2. On the **Application Logs** page, click **Purge**.
3. To delete entries by date, in the **Current and Older Than** box, enter a date.

   CAUTION: If you do not select a date, then all entries with the selected severity level(s) are deleted.
4. To delete entries by severity level, select **Information**, **Warning**, or **Critical.**

   CAUTION: If you do not select a severity level, then all entries older than the selected date are deleted.
5. Click **Apply**.

   NOTE: You must enter date and select severity level to delete log entries based on date and severity.

Networks

ASM manages LAN (private, public, and hypervisor management), hypervisor migration, hypervisor cluster private, OS Installation, File Share, and SAN (iSCSI) networks.

To facilitate network communication, you can add ranges of static IP addresses that ASM assigns to resources for iSCSI initiators. You can also create virtual identity pools of MAC, IQN, WWPN, and WWNN virtual identities that ASM assigns to virtual NICs.

NOTE: When the OS Installation network is set to Static, OS Installation is supported only for installing Linux, ESXi, and Windows on bare-metal systems with Intel NICs.

Also, make sure that the following network pre-requisites are met:

- The virtual appliance is able to communicate with the out-of-band management network.
- The virtual appliance is able to communicate with the OS Installation network in which the appliance is deployed.
- The virtual appliance is able to communicate with the hypervisor management network.
- The DHCP server is fully functional with appropriate PXE settings to PXE boot images from ASM or Razor in your deployment network.

Related links

Networking
Defining or editing existing network
Deleting a network

Networking

The **Networks** page displays information about networks defined in ASM, including:

- **Name**
- **Description**
- **Network Type**
- **VLAN ID**
- **IP Address Setting**
- **Starting IP Address**
- **Ending IP Address**
- **IP Addresses in Use**

NOTE: IP Address in Use indicates number of IPs are in use out of available IPs.

On the **Networks** page, you can:

- Define or edit an existing network. For more information on defining or editing an existing network, see Defining or editing existing network.
- Delete an existing network. For more information on deleting an existing network, see Deleting a network.
- Click **Export All** to export all the network details to a .csv file.
- Export network details for a specific network. To export the specific network details, select a network, and then click **Export Network Details**.

Also, you can click a network to see the following details in the **Summary** tab:

- Name of the user who created and modified the network.
- Date and time that the network was created and last modified.

NOTE: To sort the column by network names, click the arrow next the column header. You can also refresh the information on the page.

If you select a network from **Networks** list under **Settings**, the network details are displayed.

For a static network following information is displayed:

- **Subnet Mask**
- **Gateway**
- **Primary DNS**
- **Secondary DNS**
- **DNS Suffix**
- **Last Updated By**
- **Date Last Updated**
- **Created By**
- **Date Created**
- **Static IP Details**

For a DHCP network following information is displayed:

- **Last Updated By**
- **Date Last Updated**
- **Created By**
- **Date Created**

You can filter the IPs by selecting any of the following options from the **View** drop-down menu, under the **Static IP Address Details** section:

- **ALL IP Addresses**
- **IP Addressees in Use**
- **Available IP Addresses**

NOTE: You can also select the links under the IP Addresses in Use column. The IPs are automatically filtered based on the IP addresses In Use criteria.

Related links

Network types
Defining or editing existing network
Deleting a network

Defining or editing existing network

Adding the details of an existing network enables ASM to automatically configure chassis, servers, and I/O modules that are connected to the network.

To define or edit an existing network:

1. On the home page, click **Settings**, and then click **Networks**.
   The **Networks** page is displayed.
2. Perform one of the following:
   - To define a network, click **Define**.
     The **Define Network** page is displayed.
   - To edit an existing network, select the network that you want to modify, and click **Edit**. The **Edit Network** page is displayed.
3. In the **Name** field, type the name of the network.
4. Optionally, in the **Description** field, type a description for the network.
5. From the **Network Type** drop-down list, select one of the following network types. For more information about network types, see Network Types
   - Private LAN
   - Public LAN
   - SAN [Software iSCSI]
   - Hypervisor Management
   - Hypervisor Migration
   - Hypervisor Cluster Private
   - OS Installation
   - Fileshare
   - FIP Snooping
   - VSAN
   - Hardware Management

NOTE: The virtual MAC identity that ASM assigns to the NIC depends on the network type selected when adding a network.

- For a LAN network type, a virtual MAC address is assigned to the server.
- For an iSCSI network type, a virtual iSCSI MAC address is assigned to the server.

6. In the **VLAN ID** field, type the VLAN ID between 1 and 4094.

NOTE: ASM uses the VLAN ID specifically to configure I/O modules to enable network traffic to flow from the server to configured networks during deployment.

NOTE: The VLAN ID can be edited only if the network is not currently referenced by a template.

7. Select **Configure static IP address ranges** check box, and then do the following:

NOTE: After a network is created, you cannot select or clear the Configure static IP address ranges check box to configure static IP address pools.

a. In the **Gateway** field, type the default gateway IP address for routing network traffic.
b. In the **Subnet Mask** field, type the subnet mask.
c. Optionally, in the **Primary DNS** and **Secondary DNS** fields, type the IP addresses of primary DNS (required) and secondary DNS (optional).
d. Optionally, in the **DNS Suffix** field, type the DNS suffix to append for host name resolution.
e. Click **Add IP Range**, type a **Starting IP Address** and **Ending IP Address**, and then click **Save IP Range**. Repeat this step to add multiple IP address ranges based on the requirement.

NOTE: The IP address ranges cannot overlap. For example, you cannot create an IP address range of 10.10.10.1–10.10.10.100 and another range of 10.10.10.50–10.10.10.150.

NOTE: The network type can be edited only if the network is not currently referenced by a template.

8. To define the network configuration, click **Save**.

Related links

Network types

Network types

Using ASM, you can manage the following network types.

- **Private LAN** — Used to access network resources for functions such as vMotion traffic or heartbeat communication.
- **Public LAN** — Used to access network resources for basic Networking activities.

NOTE: Private and public LANs are functionally identical in ASM. The purpose of offering both labels is to help users categorize LANs based on functional use.

- **SAN (iSCSI)** — Used to manage storage-related traffic on an iSCSI network. If an IP address pool is associated with the network, then ASM can use it to configure the iSCSI initiator IP address when doing a SAN (iSCSI) boot. Static or DHCP.
- **Hypervisor Management** — Used to identify the management network for a hypervisor or operating system deployed on a server.
- **Hypervisor Migration** — Used to manage the network that you want to use for live migration. Live migration allows you to move running virtual machines from one node of the failover cluster to different node in the same cluster.
- **Hypervisor Cluster Private** — Used for private cluster heartbeat network communication.
- **OS Installation** — Allows static or DHCP network for OS imaging on servers.

NOTE: When the OS Installation network is set to Static, OS Installation is supported only for installing Linux, ESXi, and Windows on bare-metal systems with Intel NICs.

- **Fileshare** — Used to manage the NFS traffic in the NetApp Storage file system.
- **Hardware Management** — Used for out-of-band management of hardware infrastructure.
- The FIP VLAN Request is multicast to the destination MAC Address of ALL-FCF-MACs. The Source Address for the VLAN Request is the ENode MAC and it is important to note that the frame is transmitted without an 802.1Q (VLAN) tag

VLAN ID

A VLAN ID is a unique identifier that enables switching and routing of network traffic.

The VLAN ID must be a number between 1 and 4094. If using a flat network (no VLANs), type a value of 1.

Deleting a network

NOTE: You should not delete a network that is referenced in a template. This affects the services that are deployed using this template.

To delete a network:

1. On the home page, click **Settings**, and then click **Networks**.
   The **Networks** page is displayed.
2. Click the network that you want to delete, and then click **Delete**.
3. Click **OK** when the confirmation message is displayed.

Related links

Defining or editing existing network

Repositories

On the repositories page, you can perform the following operations:

- **OS Image Repositories** tab — Enables you to create OS image repositories.
- **Firmware/Software Repositories** tab — Enables you to upload firmware and software repositories.

The **OS Image Repositories** tab displays the following information:

- **State** — Displays the following states:
  - Available — Indicates that the OS image repository is downloaded and copied successfully on the appliance.
  - Pending — Indicates that the OS image repository download process is in progress.
  - Error — Indicates that there is an issue downloading the OS image repository.
- **Repository** — Display the name of the repository.
- **Image Type** — Displays the operating system type.
- **Source Path** — Displays the share path of the repository in a file share.
- **In Use** — Displays the following options:
  - **True** — Indicates that the OS image repository is in use.
  - **False** — Indicates that the OS image repository is not in use.
- **Available Actions** — Select any one of the following options:
  - **Delete**
  - **Edit**
  - **Resynchronize**

NOTE: You cannot perform any actions on repositories that are in use. However, you can delete repositories that are in an Available state but not in use.

NOTE: All the options are available only for repositories in an Error state.

From this page, you can:

- Click **Add** to add a new repository.
- Select a repository from the list and click **Remove** to remove a repository.

Related links

Types of firmware repositories
Understanding Firmware/Software Repositories tab

Adding OS Image repositories

To add an OS image repository:

1. On the **Repositories** page, click **OS Image Repositories** tab, and then click **Add**.
2. In the **Add OS Image Repository** dialog box, enter the following:
   a. In the **Repository Name** box, enter the name of the repository.
   b. In the **Image Type** box, enter the image type.
   c. In the **Source Path and Filename** box, enter the path of the OS Image file name in a file share.

      To enter the CIFS share, see the format used in the following example: **\\192.68.2.1\lab\isos\Windows2012r2.iso**

      To enter the NFS share, see the format used in this following example: **192.68.10.1:var/infs/linux.iso**
   d. If you are using the CIFS share, enter the **User Name** and **Password** to access the share.

Editing OS image repository

To edit the OS image repository:

1. On the home page, click **Settings**, and then click **Repositories**.
2. From the **Available Actions** drop-down menu, click **Edit** for a repository in an **Error** state.
   The **Edit OS Image Repository** page is displayed.
3. Edit the **Source Path and Filename** and type the user credentials.

   NOTE: You cannot modify the Repository Name and Image Type.
4. Click **Save**.

Resynchronizing OS image repository

You can use the resynchronize option to restore the OS image from the database after a backup and restore.
To resynchronize the OS image repository:

1. On the home page, click **Settings**, and then click **Repositories**.
2. From the **Available Actions** drop-down menu, click **Resynchronize** for a repository in an **Error** state.
   The **Resynchronize OS Repository** page is displayed.
3. Type the user credentials and click **Test Connection** to test the network connection.

   NOTE: You cannot edit the Source Path and Filename.
4. Click **Resynchronize**.
   The repository state changes to Copying state.

Understanding Firmware/Software Repositories tab

The **Firmware/Software Repositories** tab displays the following information about the firmware repositories:

- **Repository Name** — Displays the name of the repository.
- **Source** — Displays the path of the repository that contains the catalog file.

Select the repository to view the following information about firmware package:

- **Bundles** — Displays the number of bundles available in the firmware catalog.
- **Components** — Displays the number of firmware software components available in the firmware catalog.
- **Created On** — Displays the date when the repository is created.
- **Last Updated** — Displays the date when the repository last updated.

- **Services Affected** — Displays the services in which the firmware catalog is used.

From this page, you can:

- Add new repository
- Select a repository from the list, and click the delete icon in the same row to remove the repository.

  NOTE: If you remove a repository, the repository is deleted from the appliance not from the file share.

  NOTE: The embedded repository may not be removed
- Select a repository from the drop-down list, to set a repository as the default firmware repository
- Select a repository from the list, in the right pane, click **View Bundles** to view the firmware and software bundles available in the repository.
- Select a repository from the list, in the right pane, click **Add Custom Bundle** to add custom firmware file to the repository.

Related links

Adding firmware repositories

Viewing firmware and software bundles details

Adding firmware repositories

1. On the **Repositories** page, click **Add Firmware Repository**.
2. In the **Add Firmware Repository** dialog, select one of the following options:
   - **Import ASM's recommended repository from ftp.dell.com** — Select this option to import the firmware repository that contains the firmware bundles recommended for ASM.
   - **Load repository from network path** — Select this option to upload the repository from any one of the following file shares NFS, CIFS, FTP, and HTTP.
   - **Load repository from local drive** — Select this option to upload the repository from local system.
3. If you selected **Load repository from network path**, perform the following:
   - In the **File Path** box, enter the location of the catalog file. Use on of the following formats:
     - NFS share for xml file: host:/share/filename.xml
     - NFS share for gz file: host:/share/filename.gz
     - CIFS share for xml file: \\host\share\filename.xml
     - CIFS share for gz file: \\host\share\filename.gzb
     - FTP share for xml file:ftp://host/share/filename.xml
     - FTP share for gz file:ftp://host/share/filename.gz
     - HTTP share for xml file:http://host/share/filename.xml
     - HTTP share for gz file:http://host/share/filename.gz
   - If using a CIFS share, enter the **User Name** and **Password**.
4. If you selected **Load repository from local drive**, click Browse, and select the catalog file.
5. Click **Save**.

Types of firmware repositories

There are three types of firmware repositories:

NOTE: Only devices validated against the embedded or default repository are displayed on the Resources page.

- **Embedded ASM Firmware Repository** — ASM ships with an Embedded Firmware Repository that contains a subset of the minimum firmware versions that are supported by ASM for the management interfaces of Dell hardware.

  This embedded catalog is not a full catalog. If a full catalog is not downloaded, the firmware level of all devices discovered in ASM are validated against the firmware level listed in the embedded firmware repository. Compliance to this Repository can be viewed on the Resources page.

NOTE: Devices with firmware levels below the minimum firmware listed in the embedded ASM firmware repository are marked as Upgrade Required.

- **Default Firmware Repository** — This is the Default Firmware Repository. This repository is applied to all devices that are either not in a Service or are part of Services that do not have a Service Level Firmware Repository.

  To set a default firmware repository, you must download a catalog either from **Dell.com** or from an internal share through the ASM User Interface. The Embedded Repository is no longer used if a Default Firmware Repository is set. Compliance to this Repository can be viewed on the Resources page.

  NOTE: Devices with firmware levels below the minimum firmware listed in the default repository are as Non-Compliant (out of compliance).

- **Service Level Firmware Repository** — This repository is applied only to Servers that are in Service and to which the Service Level Firmware Repository is assigned.

  NOTE: Devices with firmware levels below the minimum firmware level listed in service level repository are marked as Non-Compliant. When a Service Level Firmware Repository is assigned to a Service, the firmware validation is checked only against the Service Level Firmware Repository and the Default Firmware Repository checks are no longer applied to the devices associated with this Service.

Viewing firmware and software bundles details

The following are the steps to view the firmware and software bundles details:

1. On the home page, click **Settings**, and then click **Repositories**.
2. Click the **Firmware/Software Repositories** tab, select a repository, and then click **View Bundles**.
   A list of system and software bundles is displayed.
3. Click **System Bundles** to view the firmware or system bundles.
4. Click **Software Bundles** to view the software bundles.

You can see the following information regarding bundles:

- Name — Displays the name of the firmware or software update package.
- Version — Displays the version of the firmware or software update package.
- Date — Displays the date when the firmware or software update package was downloaded.

NOTE: You cannot create a catalog from start in ASM. You have to create a base catalog in DRM tool and then you can upload that to ASM. You can select the uploaded catalog and add bundles in it using Add Bundle feature.

Adding Custom Bundle

Add Custom Bundle feature allows you to add firmware bundles to an imported catalog. Previously you were only allowed to import catalogs, but now you can add firmware bundles to the existing catalogs to ensure firmware compliance and update firmware when required. Perform the following steps to use this feature:

1. Click **Settings** on the Getting Started page.
2. Under **Settings**, click **Repository**
3. On **Repository** page, click **Firmware**.
4. Select a catalog from the page, in which you want to add bundle. After that, Click **Add Custom Bundle** top right corner of the same page.
5. An **Add Custom Bundle** window is displayed.
   a. Enter the custom bundle's name in **Name** field.
   b. Enter the custom bundle's description in **Description** field.
   c. Enter the custom bundle's version in **Version** field.
   d. Select device type from **Device Type** drop-down menu.

NOTE: If you select switch from Device Type drop-down menu, version should include parenthesis. For example: 9.7(01).

e. Select device model from **Device Model** drop-down menu.

f. You can select priority either as **Urgent**, or **Recommended** or else **Optional** from **Criticality** drop-down menu.

g. Click **Browse** button beside **Upload Firmware** option. Browse and select firmware file, click **Open**.

h. Click **Save**.

After you perform the tasks, the firmware file will get uploaded with the bundle.

NOTE: Adding custom bundles is applicable only for firmware update.

NOTE: If you do not want to add firmware file, then you can perform only compliance check.

NOTE: You cannot create a catalog from scratch in ASM. You have to create a base catalog in DRM tool and then you can upload that to ASM. You can select the uploaded catalog and add bundles in it using Add Bundle feature.

Jobs

NOTE: User with Administrator role can only view the jobs.

In ASM, you can view the details of the following jobs:

- Discovery
- Firmware Update
- Inventory
- Service Deployment
- Chassis Configuration

The **Jobs** page displays the following information about the jobs that are scheduled or currently running in ASM:

- **State** — Displays one of the following states based on the job status:
  - **Error** — Job has completed with errors (job is complete but failed on one or more resources)
  - **Scheduled** — Job is scheduled to run at a specific time. It can be scheduled to run at a single time or at several times as a recurring job.
  - **In progress** — Job is running.
- **Job Name** — Identifies the name of the job.
- **Started By** — Displays the name of the user who started the job.
- **Start Time** — Displays the date and time when the job is scheduled to run.
- **Time Elapsed** — Displays the time elapsed from the start time to the end time of a job instance.

NOTE: If a job scheduled is a one-time job, after execution, it will not be listed in the Jobs page.

Users

The **Users** page allows you to manage the users within ASM. You can create a user, or edit, delete, enable, disable or import existing users from Active Directory.

The **Users** page displays the following information about users:

- User Name
- Domain
- Role

- Last Name
- First Name
- State (*Enabled* or *Disabled*)

On this page, you can:

- Click refresh icon on the top left of the **Users** tab to retrieve the newly added users.
- Edit or delete an existing user.
- Create local user.
- Enable or disable a user account.
- Import Active Directory Users.

Also, you can click the specific user account to view the following user-related information:

- Email
- Phone
- Directory Services

NOTE: You can also refresh the information on the page. To sort the users list based on the entries in a column, click the arrow next the column header.

Creating a user

The Create option allows you to create an ASM user. Enter the following information to create a user.

1. On the home page, click **Settings**, and then click **Users**.
2. On the **Users** page, click **Create**.
3. Enter a unique **User Name** to identify the user account.
4. Enter a **Password** that a user enters to access ASM. Confirm the password.

   NOTE: The password length must be between 8–32 characters and must include at least one number, one capital letter, one lowercase letter.
5. Enter the user's **First Name** and **Last Name**.
6. From the **Role** drop-down list, select one of the following roles:
   - **Administrator**
   - **Standard**
   - **Read only**
7. Enter the **Email** address and **Phone** number for contacting the user.
8. Select **Enable User** to create the account with an *Enabled* status, or clear this option to create the account with a *Disabled* status.
9. Click **Save**.

Related links

Users
Editing a user
Deleting a user
Enabling or disabling users
Importing Active Directory Users

Deleting a user

The Delete option allows you to remove an existing ASM user. Perform the following tasks to delete a user:

1. On the home page, click **Settings** and then click **Users**.
2. On the **Users** page, select one or more user accounts to delete.
3. Click **Delete**.
   Click **Yes** in the warning message to delete the account(s).

Editing a user

The Edit option allows you to edit an ASM user profile. Perform the following tasks to edit a user profile:

1. On the home page, click **Settings**, and then click **Users**.
2. On the **Users** page, select a single user account which you require to edit.
3. Click **Edit**.

   NOTE: For security purpose, please confirm your password before editing the user.
4. You can modify the following user account information from this window:
   - **First Name**
   - **Last Name**
   - **Role**
   - **Email**
   - **Phone**
   - **Enable User**

   NOTE: If you select the Enable user check box, user is able to log in to ASM. If you disable the check box, user will not able to log in to ASM interface.
5. Click **Save**.

Related links

Users
Creating a user
Deleting a user
Enabling or disabling users
Importing Active Directory Users

Enabling or disabling users

The **Enable** option allows you to change the user account state to *Enabled* and the **Disable** option allows you to change the user account state to *Disabled*. Perform the steps following to enable or disable the user account state:

1. On the home page, click **Settings**, and then click **Users**.
2. On the **Users** page, select one or more user accounts to enable/disable.
3. In the menu, click **Enable** or **Disable**, to update the State to Enabled or Disabled, as selected.

   NOTE: For an already *Enabled* user account State, the Enable option in the menu is deactivated, and for an already *Disabled* user account State, the Disable option in the menu is deactivated.

Directory services

The Directory Services functionality allows you to create Directory Service that ASM can access for importing remote users.

On this page, you can:

- Create a Directory Service.
- Delete a Directory Service.
- Edit a Directory Service.

Directory services

The **Directory Services** option allows you to add, edit or delete an Active Directory using the **Directory Services** functionality. ASM can access these active directories to import users.

NOTE: An Active Directory user is authenticated against the specific Active Directory Domain that a user belongs to.

NOTE: While logging in to the ASM software, the Active Directory user is required to first enter the directory name that a user belongs to, followed by the username, for example: domain\username.

The **Directory Services** page displays the following information about the ASM active directories:

- Host IP address
- Name
- Directory Type

From this screen, you can:

- Add a directory service.
- Edit or Delete an existing directory service.

Related links

Deleting a directory service
Editing a directory service

Adding a directory service

To add a Directory Service, configure the following:

- **Connection Settings**
- **Attribute Settings**

Connection settings

1. On the home page, click **Settings**, and then click **Users**.
2. In the **Directory Services** tab, click **Create**.
3. Select the directory service type from the **Type of Directory Service** drop-down list.
4. Enter the directory service name in the **Name** box.
5. Enter the **User Name**, **Password**, **Host**, **Port** and **Protocol** (*Plain* or *SSL*) of the Active Directory that is to be added to ASM.

   NOTE: The default Windows port is 389, but see your Active Directory configuration for the specific port used for your Active Directory. Currently, the only format supported for User Name is <user name>@<domain.com >.
6. Click **Next**.

Related links

Attribute settings
Connection settings matrix
Attribute settings matrix
Summary
Importing Active Directory Users

Connection settings matrix

Table 15. Connection settings matrix

Field Name	Description
Type Of Directory Service	Refers to the type of directory service (currently available, Microsoft Active Directory).
Name	Refers to the Active Directory (AD) configuration name as added in ASM. For example: mydomain
User Name	Refers to the AD account that has privileges to search for users. The account name must be entered using the User Principle Name format. For example: administrator@mydomain.com
Password	Refers to the AD server password for the account in the **User Name** box.
Host	Refers to the AD server FQDN host name or IP address. For example: 192.168.0.5
Port	Refers to the AD server port. For example: 389
Protocol	Refers to the protocol type as Plain or SSL. For example: Plain

Attribute settings

The **Attribute Settings** allows you to perform the attribute settings required for adding an Active Directory.

1. Enter the **Base DN**, **Filter**, **Username Attribute**, **First Name**, **Attribute**, **Last Name Attribute**, and the **Email Attribute** of the Active Directory that is to be added to ASM.
2. Click **Next**.

Attribute settings matrix

Table 16. Attribute settings matrix

Field Name	Description
Base DN	Refers to the Distinguished Name (DN) where the users are searched by ASM. It is the Distinguished Name (DN) of the starting point for directory server searches. For example: CN=Users,DC=mydomain,Dc=com
Filter	Refers to the filters that enable you to define search criteria. For example: objectClass=*
User Name Attribute	Refers to the Active Directory record attribute that represents the User Name attribute. This attribute is mapped to ASM User Name attribute. For example: sAMAccountName
First Name Attribute	Refers to the Active Directory record attribute that represents First Name. This attribute is mapped to ASM First Name attribute. For example: givenName
Last Name Attribute	Refers to the Active Directory record attribute that represents the Last Name of the user. This attribute is mapped to ASM Last Name attribute. For example: sn
Email Attribute	Refers to the Active Directory record attribute that represents the Email of the user. This attribute is mapped to ASM Email attribute. For example: mail

Summary

The **Summary** option allows you to verify the entered connection and attribute settings before committing the settings. Perform the required steps as mentioned below:

1. To change the **Connection Settings** or the **Attribute Settings**, click **Back**.
2. To create the directory services with the existing settings, click **Save**.

Related links

Attribute settings
Connection settings

Editing a directory service

The **Edit** option allows you to edit the existing directory settings. Perform the following steps to edit the active directory settings:

1. On the home page, click **Settings**, and the click **Users**.
2. In the **Directory Services** check box, select a single directory service to be edited by checking the required service directory check box.
3. Edit the **Connection settings**, as necessary.
4. Edit the **Attribute Settings**, as necessary.
5. Review the **Summary** and edit settings. (Optional).
6. Click **Save** to update the edited settings.

Related links

Deleting a directory service

Deleting a directory service

The **Delete** option allows you to delete a directory service. Perform the following steps to delete a directory service:

1. On the home page, click **Settings**, and then click **Users**.
2. In the **Directory Services** tab, select a single or multiple directory services to be deleted, by checking the required service directory check boxes.
3. Click **OK** in the warning message window to delete the selected directory services.

Related links

Editing a directory service

Importing Active Directory Users

The **Import Active Directory Users** option allows you to import various active directory users into ASM. Perform the following tasks to import the users into ASM:

NOTE: Prior to importing Active Directory users, you must create at least one directory service using ASM. After importing the users, these users can log in to ASM virtual appliance using the following format: <ASM Directory Service Name>/ <user name>, and then type the password.

NOTE: If an imported user is deleted from Active Directory, that user is not automatically deleted from ASM. The deleted user cannot log in to the virtual appliance, and you must remove the user manually from the user list.

NOTE: Importing an already imported user does not have any effect. The user role also remains the same.

1. Click **Settings**, and then click **Users**.
2. Under **Users** tab, click **Import Active Directory Users**.

   The **Import Active Directory Users** page is displayed.
3. Select a specific directory source from the **Directory Source** drop-down list to import the users from the selected directory source.
4. Under the **Available Users/Groups** section, type a user or group name in the **Find a User/Group** field to search for a user or group in the selected directory.

NOTE: You can select any one of the following options from the View drop-down menu to filter the search results:

- **All** — displays both users and groups
- **Users**— displays only users
- **Groups** — displays only groups

5. Select the users or group you want to import and click the forward arrow **(>>)** button.
   The selected users or groups are added to the **Users/Groups to the imported** section.
6. To assign a role to all the users or groups, select the users or groups and select any one of the following roles from the **User Role** drop-down menu:
   - **Read Only**
   - **Standard**
   - **Administrator**

NOTE: To apply specific roles, select the role from the Role drop-down menu beside the user or group name.

NOTE: You can view the imported group by selecting the All Groups from the Filter by Group drop-down menu.

NOTE: In a single import operation, if you import a user individually and as part of group, the role assigned to the user individually precedes the role assigned to the group.

NOTE: While importing Active Directory users, ASM roles are not automatically mapped to Active Directory user roles. Therefore, it is important to assign an appropriate role to each imported user.

About roles

Every ASM user account can be assigned to any one of the following roles:

- Administrator — Users with Administrator role have the privilege to view all the pages and to perform all operations in ASM and grant permission to Standard users to perform certain operations.
- Standard — Users with Standard role can view certain pages and perform certain operations based on the permission granted by Administrator. Also, Standard users can grant permission to other users to view and perform certain operations they own.
- Read Only — Users with Read Only role can view all ASM operations but are not allowed to perform any operations. When a user logs in as a Read Only user, ASM does not allow the user to perform any operations by deactivating the functionality on the UI.

The following table describes the privileges or permissions associated with the roles:

Table 17. About roles

Feature	Permission	Roles		
		Administrator	Standard	Read-only
Dashboard	View	Yes	Owner/ Participant	Yes

			NOTE: Standard users who are granted permission or are owners, can view the dashboard data and links to services, templates, resource utilization, and resource pools. However, the data is filtered by services, resource utilizations and pools, recent templates, and any recent activity performed by the user as an owner or participant.	
	Read	Yes	Owner/ Participant	Yes
	Link to other pages	Yes	Owner/ Participant	Yes **NOTE: Direct links to deploy a service from recent templates is disabled.**
Services	View	Yes	Owner/ Participant **NOTE: Users can view only services that they own or are granted permission to.**	Yes
	Deploy a Service	Yes	Owner/ Participant **NOTE: Users can only deploy services they own or are granted permission to.**	No
	Export to File	Yes	Owner/ Participant **NOTE: Users can only export services they own or are granted permission to.**	No
Service Details	View	Yes	Owner/ Participant	Yes

			NOTE: On the Service page, users can view service details and perform actions only for services which they are owners or are granted permission to. Users with this role cannot perform any firmware action.	
	Open Device Console	Yes	Owner/ Participant	No
	Edit Service Information	Yes	Owner	No
	Delete	Yes	Owner	No
	Cancel	Yes	Owner	No
	Retry	Yes	Owner	No
	View All Settings	Yes	Owner/ Participant	Yes
	Export to File	Yes	Owner/ Participant	No
	Add component	Yes	Owner	No
	Migrate servers	Yes	Owner	No
	Firmware Actions	Yes	No	No
Templates	View	Yes	Participant **NOTE: Users can only view templates for which they have been granted permission to by an administrator.**	Yes
	Read template	Yes	Participant	Yes
	Create new template	Yes	No	No
	Edit template	Yes	No	No
	Delete template	Yes	No	No
	View template details	Yes	Participant	Yes
	Clone template	Yes	No	No
Template Edit	View	Yes	No	No

	Edit name/category/ description	Yes	No	No
	Publish template	Yes	No	No
	Delete template	Yes	No	No
	View All Settings	Yes	No	No
	Import template	Yes	No	No
Template Details	View	Yes	Participant	Yes
	Deploy Service	Yes	Participant	No
	Edit	Yes	No	No
	View All Settings	Yes	Participant	Yes
	Delete Template	Yes	No	No
Resources	View	Yes	Participant **NOTE: Users can view resources that part of a server pool for which they are granted permission. They can also view common and shared resources that are not part of a pool. However, users with this role can only run inventory update on the resources.**	yes
	View All Resources tab	Yes	Participant	yes
	Run Discovery	Yes	No	No
	Remove resources	Yes	No	No
	Manage or unmanage resources	Yes	No	No
	Run inventory	Yes	Participant	No
	View details (all tabs)	Yes	Participant	Yes
	Launch resource element manager (in details)	Yes	Participant	No
Server Pools tab	View	Yes	Participant	Yes

	Create	Yes	No	No
	Edit	Yes	No	No
	Delete	Yes	No	No
Firmware tab	View	Yes	Yes	Yes
	Add Repository	Yes	No	No
	Remove	Yes	No	No
	Set as Default	Yes	No	No
	Import latest	Yes	No	No
	View Bundles	Yes	Yes	Yes
Settings	View	Yes	No **NOTE: Users cannot view the Settings page.**	Yes
Application Logs	View	Yes	No	Yes
	Export All	Yes	No	No
	Purge	Yes	No	No
Backup and Restore	View	Yes	No	Yes
	Backup Now	Yes	No	No
	Restore	Yes	No	No
	Edit Settings and Details	Yes	No	No
	Edit Auto Schedule Backup	Yes	No	No
Credential Management	View	Yes	No	Yes
	Create	Yes	No	No
	Edit	Yes	No	No
	Delete	Yes	No	No
Getting Started	View	Yes	No	Yes
	• Define Networks • Discover Resources • Define Existing Services • Configure Resources	Yes	No	No

	• Publish Templates			
Networks	View	Yes	No	Yes
	Define	Yes	No	No
	Edit	Yes	No	No
	Delete	Yes	No	No
Users	View	Yes	No	Yes
	Create	Yes	No	No
	Edit	Yes	No	No
	Disable/Enable	Yes	No	No
	Delete	Yes	No	No
	Import	Yes	No	No
Directory Services	View	Yes	No	Yes
	Create	Yes	No	No
	Edit	Yes	No	No
	Delete	Yes	No	No
Virtual Appliance Management	View	Yes	No	Yes
	Generate Troubleshooting Bundle	Yes	No	No
	Edit Time Zone and NTP Settings	Yes	No	No
	Edit Proxy Settings	Yes	No	No
	SSL Certificates	Yes	No	No
	Generate Certificate Request	Yes	No	No
	Upload Certificate	Yes	No	No
	Edit License	Yes	No	No
Virtual Identity Pools	View	Yes	No	No
	Create	Yes	No	No

	Export	Yes	No	No
	Delete	Yes	No	No

Related links

Creating a user
Editing a user
Deleting a user
Enabling or disabling users
Importing Active Directory Users

Virtual appliance management

Virtual Appliance Management allows you to:

- Generate a troubleshooting bundle
- Update the ASM virtual appliance
- Edit NTP settings
- Update Repository Path
- Edit DHCP Settings
- Edit proxy server settings
- Generate and download a Certificate Signing Request (CSR) and upload the resulting SSL certificate
- Upload an ASM license

Related links

Update the ASM virtual appliance
Editing default time zone and NTP settings
Generating a certificate signing request
Downloading the certificate signing request
Uploading an SSL certificate
Editing proxy settings
License management
Editing DHCP settings

Update the ASM virtual appliance

To update the ASM virtual appliance, do the following:

1. On the home page, click **Settings**, and then click **Virtual Appliance Management**.
2. In the **Update Repository Path** section it displays if a newer version of ASM is available.

   NOTE: For more information, see Update Repository Path to configure the update repository path.
3. On the **Virtual Appliance Management** page, click **Update Virtual Appliance**.

Update Repository Path

To update the repository path, do the following:

1. After you click Update Virtual Appliance, a dialogue box is displayed with a statement and warning message.

NOTE: The message displayed in the dialogue box is " Updating the appliance restarts the system. The action will log off all current users and cancel all jobs in progress." It even displayed the message " The update process takes approximately 25 minutes depending on your data connection: 15 minutes to download the update and 10 minutes to apply." Apart from these, it gives you information about number of logged-in users, and in progress jobs. At the end, it asks for your confirmation " Are you sure you want to perform an appliance update?

2. Click **Yes** on the dialogue box to update your appliance.

NOTE: This process restarts your system. Once update and restore is complete, you get logged in again. Once the update is complete, it redirects you to the login page. In the meantime, it monitors the progress of updates and displays messages accordingly. At the end, you get a tab as Click to log in. After you click the tab, you will be directed to login page to log in again to the appliance.

Generating a troubleshooting bundle

A troubleshooting bundle is a compressed file that contains appliance logging information for ASM virtual appliance. If necessary, you must download the bundle and send it to Dell support for issue debug.

1. On the home page, click **Settings**, and then click **Virtual Appliance Management**.
2. On the **Virtual Appliance Management** page, click **Generate Troubleshooting Bundle**.
3. Open or save the file.

Generating and uploading the SSL certificates

Uploading an SSL certificate provides the following advantages:

- Ensures secure transmission by encrypting data that ASM sends over the web
- Provides authentication and ensures that data is routed to its intended endpoint
- Prevents users from receiving browser security errors

To upload an SSL certificate:

1. Generate a Certificate Signing Request (CSR).
2. Download the CSR.
3. Submit the CSR to a Certificate Authority (CA). The CA provides a valid SSL certificate.
4. Upload the SSL certificate to ASM.

Related links

Generating a certificate signing request
Downloading the certificate signing request
Uploading an SSL certificate

Generating a certificate signing request

A Certificate Signing Request (CSR) includes server information (such as domain name, locale) that certificate authorities require to provide a valid SSL certificate.

After generating the CSR, download the encrypted text, and then submit it to a certificate authority. The Certificate Authority provides a valid SSL certificate for you to upload.

1. On the home page, click **Settings**, and then click **Virtual Appliance Management**.
2. On the **Virtual Appliance Management** page, under the **SSLCertificates** section, click **Generate Certificate Signing Request**.
   a. In the **Distinguished Name (www.domain.com)** box, type a distinguished name in the format www.domain.com.
   b. In the **Business Name** box, type a business name where the certificate is recorded.
   c. In the **Department Name** box, type a department name of the organizational unit (for example, IT, HR, or Sales) for which the certificate is generated.
   d. In the **Locality (Town/City)** box, type a locality name in which the organization is located.

e. In the **State (Province/Region)** box, type a state name in which the organization is located (do not abbreviate).
f. From the **Country** drop-down list, select a country in which the organization is located.
g. In the **Email** box, type a valid email address.
h. Click **Generate**.

3. Click **Download Certificate Signing Request**, and then copy the text that is displayed. To receive a valid SSL certificate, submit this text to a certificate authority.

Downloading the certificate signing request

After generating the CSR, download the resulting text and submit it to a certificate authority. The certificate authority provides an SSL certificate for you to upload to ASM.

1. On the home page, click **Settings**, and then click **Virtual Appliance Management**.
2. In **the Virtual Appliance Management** page, under the **SSLCertificates** section, click **Download Certificate Signing Request**.
3. To receive a valid SSL certificate, copy the displayed text and then submit it to a certificate authority.

After the certificate authority provides the SSL certificate, upload it to ASM.

Uploading an SSL certificate

Before you upload an SSL certificate, generate and download a certificate signing request (CSR). To receive a valid SSL certificate, submit the CSR to a certificate authority. Save the certificate to a local network share.

1. On the home page, click **Settings**, and then click **Virtual Appliance Management**.
2. On the **Virtual Appliance Management** page, under the **SSLCertificates** section, click **Upload Certificate**.
3. Click **Browse**, and select an SSL certificate.
4. To upload the certificate, click **Save**.
5. Confirm or cancel the action when a confirmation message is displayed.

After uploading the certificate, the GUI becomes unavailable as the web services are restarted, the virtual appliance shell is still accessible and all active users are logged out.

Editing DHCP settings

If you have already configured a DHCP server on the ASM appliance, you can edit the DHCP server settings on the **Virtual Appliance Management** page.

To edit the DHCP server settings:

1. On the **Virtual Appliance Management** page, under the **DHCP Settings** section, click **Edit**.
2. In the DHCP Settings dialog box, modify the setting as needed. For more information on configuring the DHCP settings, see Configure DHCP Settings

Related links

Configure DHCP settings

Editing proxy settings

If your network uses a proxy server for external communication, then you must type the critical information to enable communication with ASM virtual appliance.

1. On the home page, click **Settings**, and then click **Virtual Appliance Management**.
2. On the **Virtual Appliance Management**, under the **Proxy Settings** section, click **Edit**.
3. Select **Use HTTP Proxy Settings**.
4. In the **Server Address (IP or Hostname)** box, type a server address for the proxy server.
5. In the **Port** box, type a valid port number from 1–65535. Commonly used ports for a proxy server are 80 and 8080.
6. If the proxy server requires credentials to log in, select **Use Proxy Credentials** and then in **User Name** and **Password** boxes, type the required user name and password. To verify the password, type the password in **Confirm Password**.

7. To validate the settings typed on this page, click **Test Proxy Connection**.
8. Click **Save**.

License management

ASM licensing is based on the total number of managed resources.

The valid license type supported is Standard license. Standard license is a full-access license type. After uploading an initial license, you can upload subsequent licenses on the **Virtual Appliance Management** page. Subsequent uploads replace the existing license.

1. On the home page, click **Settings**, and then click **Virtual Appliance Management**.
2. On the **Virtual Appliance Management** page, under the **License Management** section, click **Add**. **License Management** window is displayed.
3. Click **Browse** button beside **Upload License** and select an Evaluation license file, and then click **Open**.

   You get information regarding license type, number of resources and expiration date of the uploaded license. on **License Management** window.
4. Click **Save** to apply the evaluation license.

   After uploading the license file, the following information about the license is displayed:

   - License Type
   - Number of Resources
   - Number of Used Resources
   - Number of Available Resources
   - Expiration Date
5. To replace the Evaluation license with standard license click the same **Add** button under **License Management** section, click **Browse** button beside **Upload License** and select a regular standard license file, and then click **Open**.

   You get information regarding license type, number of resources and expiration date of the uploaded license. on **License Management** window.
6. Click **Save** to apply the standard license,

   It replaces the evaluation license with standard license.

   After uploading the license file, the following information about the license is displayed:

   - License Type
   - Number of Resources
   - Number of Used Resources
   - Number of Available Resources

   You can add multiple standard licenses. In that scenario, details of all the licenses are displayed together under **License Management** section on **Virtual Appliance Management** page.

   NOTE: If you try to upload the same standard license second time, you get an error message stating that License has already been used.

Editing default time zone and NTP settings

Changes on this page affect the time zone and NTP server(s) that are applied to ASM virtual appliance. All time data is stored in UTC format, and is used to display log and event time stamps.

1. On the home page, click **Settings**, and then click **Virtual Appliance Management**.
2. On the **Virtual Appliance Management** page, under the **Time Zone and NTP Settings** section, click **Edit**.
3. From the **Time Zone** drop-down list, select a time zone.
4. Type the IP address or hostname in **Preferred NTP Server** and **Secondary NTP Server (optional)** for time synchronization.
5. Click **Save**. The GUI becomes unavailable as the web services are restarted, the virtual appliance shell is still accessible and all active users are logged out.

Updating repository path

By default, it comes with a repository path. To update the repository path, perform the following tasks:

1. Click **Settings**, click **Virtual Appliance Management** under **Settings**.
   Virtual Appliance Management page is displayed
2. Click **Edit** beside **Update Repository Path** option.
3. **Update Repository Path** window is displayed. You can update the path using **Update Repository Path** field.
4. Click **Save** to save the updated path.
5. It directs you to **Virtual Appliance Management** page. On the page, under **Update Repository Path**, you get the updated information regarding **Current Virtual Appliance Version**, **Available Virtual Appliance Version**, **Repository Path**
6. To perform the update, click **Update Virtual Appliance**.
7. After you click **Update Virtual Appliance**, a dialogue box is displayed with few statement and warning message.

   NOTE: The message displayed in the dialogue box is " Updating the appliance restarts the system. The action will log off all current users and cancel all jobs in progress." It even displayed the message " The update process takes approximately 25 minutes depending on your data connection: 15 minutes to download the update and 10 minutes to apply." Apart from these, it gives you information about number of logged-in users, and in progress jobs. At the end, it asks for your confirmation " Are you sure you want to perform an appliance update?"
8. After reading the message, if you decide that it's good to proceed with update virtual appliance, click **Yes** on the dialogue box.

It updates your appliance.

NOTE: This process restarts your system. Once update and restore is complete, you will be logged in again. Once the update process is complete, it redirects you to a login page. In the meantime, it monitors the progress of the update and messages you accordingly. At the end, you get a tab stating Click to log in. After you click the tab, you will be directed to a login page to log in again to the appliance.

Adding Dell ASM Service Tag

To add Dell ASM Service Tag:

1. On the home page, click **Settings**, and then click **Virtual Appliance Management**.
2. Under **Dell ASM Service Tag**, click **Edit**, type Dell ASM Service Tag, and click **Save**.

Virtual identity pools

In ASM, virtual identity pools provide a conceptual way to categorize the virtual identities that help in network communication.

A virtual identity pool can include any combination of following virtual identities:

- MAC
- IQN
- WWPN
- WWNN

By default, virtual identities that are not assigned to any virtual identity pool are automatically assigned to the *Global* pool.

After creating a virtual identity pool, you can assign the virtual identity pool to one or more templates. For example, you might create a virtual identity pool to use for specific business units, such as Finance, Human Resource, and for any specific application.

The **Virtual Identity Pools** page displays the following information about the virtual identity pools that are configured in ASM:

- **Name** — Displays the name of the virtual identity pool.

- **Description** — Displays the description to identify the virtual identity pool.
- **Created By** — Displays the name of the user who created the virtual identity pool.
- **Created Date** — Displays the time that the virtual identity pool was created and last modified.

In the **Virtual Identity Pools** page, click an existing virtual identity pool to see the following information about the virtual identity pools in the **Summary** tab:

- **Selected Prefix** — Displays the prefix that is added to the beginning of the virtual identities.
- **Reserved** — Displays the total number of virtual identities reserved for future use.
- **Assigned** — Displays the total number of virtual identities assigned to the resources.
- **Available** — Displays the total number of virtual identities available in the virtual identity pool.
- **Auto Generate** — Indicates whether auto generate virtual identity pools option is enabled or disabled.

To edit the virtual identity pools information, click **Update Pool Identities** at the bottom of the **Summary** tab.

On the **Virtual Identity Pools** page, you can:

- Create virtual identity pools
- Export virtual identity pools
- Delete virtual identity pools

Related links

Creating virtual identity pools

Creating virtual identity pools

The **Create Virtual Identity Pool** wizard enables you to create virtual identity pools and add virtual identities to the virtual identity pools.

To create a virtual identity pool:

1. On the home page, click **Settings**, and then click **Virtual Identity Pools**.
2. In the **Virtual Identity Pools** page, click **Create**.

   The **Create Virtual Identity Pool** wizard is displayed.
3. On the **Pool Information** page, type the **Pool Name** and **Pool Description** to identify the virtual identity pool, and then click **Next**.

   The virtual identity pool name must be fewer than 100 characters.
4. On the **Virtual MAC** page, add the virtual MAC identities, and then click **Next**.
5. On the **Virtual IQN** page, add the virtual IQN identities, and then click **Next**.
6. On the **Virtual WWPN** page, add the virtual WWPN identities, and then click **Next**.
7. On the **Virtual WWNN** page, add the virtual WWNN identities, and then click **Next**.
8. On the **Pool Summary** page, click **Finish**.

Related links

Adding virtual MAC identities
Adding virtual IQN identities
Adding virtual WWPN identities
Adding virtual WWNN identities

Adding virtual MAC identities

1. On the **Virtual MAC** page of the Create Virtual Identity Pool wizard, in the **Number of Virtual MAC Identities** boxes, type the total number of virtual MAC identities that you want to add (any whole number between 1 and 1,024).
2. From the **MAC Address Prefix** list, type the MAC address prefix to be added to the starting of the MAC addresses.

3. Select **Auto Generate Identities if needed during deployments** check box to automatically generate the Virtual MAC address during the deployment, if necessary.

Adding virtual IQN identities

You can add from 1 to 1024 virtual WWPN identities at one time. The maximum number of virtual WWPN identities that ASM can manage is 16,000.

1. On the **Virtual IQN** page of the Create Virtual Identity Pool wizard, in the **Number of Virtual iSCSI Identities** boxes type the total number of virtual IQN identities that you want to add (any whole number between 1 and 1,024).
2. In the **IQN Prefix** box, type the IQN prefix that to be added at the starting of the IQN.

   Examples of possible prefixes include product types, serial numbers, host identifiers, and software keys.

   NOTE: The IQN prefix cannot exceed 213 characters, must contain only alphanumeric characters (uppercase and lowercase), and the following special characters: – _, ,: .
3. Select **Auto Generate Identities if needed during deployments** check box to automatically generate the Virtual IQN addresses during the deployment, if necessary.

Adding virtual WWPN identities

You can add from 1 to 1024 virtual WWPN identities at one time. The maximum number of virtual WWPN identities that ASM can manage is 16,000.

1. On the **Virtual WWPN** page of the Create Virtual Identity Pool wizard, in the **Number of Virtual WWPN Identities** boxes, type the total number of virtual WWPN identities that you want to add (any whole number between 1 and 1,024).
2. From **WWPN Prefix** drop-down list, select the WWPN prefix to be added to the starting of the WWPN.
3. Select **Auto Generate Identities if needed during deployments** check box to automatically generate the Virtual WWPN addresses during the deployment, if necessary.

Adding virtual WWNN identities

You can add from 1 to 1024 virtual WWNN identities at one time. The maximum number of virtual WWNN identities that ASM can manage is 16,000.

1. On the **Virtual WWNN** page of the Create Virtual Identity Pool wizard, in **Number of Virtual WWNN Identities** type the total number of virtual WWNN identities that you want to add (any whole number between 1 and 1,024).
2. From the **WWNN Prefix** drop-down list, select the WWNN prefix to be added to the starting of the WWNN.
3. Select **Auto Generate Identities if needed during deployments** check box if you want to automatically generate the Virtual WWNN addresses during the deployment.

Deleting virtual identity pools

NOTE: You cannot delete a *Global* virtual identity pool, and you cannot delete the virtual identity pools that are currently associated with a template or if the virtual identity pools contain identities in an `Assigned` or `Reserved` state.

1. On the home page, click **Settings**, and then click **Virtual Identity Pools**.
2. On the **Virtual Identity Pools** page, select the check boxes next to the virtual identity pools that you want to delete, and then click **Delete**.
3. Click **OK** when the confirmation message is displayed.

Exporting virtual identity pools

You can export the .txt file that contains the virtual identity pools information.

1. On the home page, click **Settings**, and then click **Virtual Identity Pools**.
2. On the **Virtual Identity Pools** page, select the virtual identity pools detail that you want to export, and then click **Export**.
3. Open or save the file.

9

Troubleshooting

This topic includes details for resolving common issues encountered in ASM 8.3.

LC operation times out while deploying server profile to a server

While updating the server configuration using config XML, the LC job remains in the RUNNING state and eventually gets timed out. This is observed in case there is "bootseq" attribute in the request XML. This is identified as an issue in LC and fix for this is available along with 13G.

To resolve this issue, remove the content "bootseq" attribute from the config XML.

Hyper-V host deployments using network storage only support certain configurations

Currently, while deploying Hyper-V, exactly two EqualLogic storage volumes using IP/IQN authentication are required. For Hyper-V, CHAP authentication is not supported.

iSCSI storage network only support static IP addressing

Currently, while creating a network in ASM for iSCSI connectivity, specify the network using static IPs. Setting an iSCSI network to DHCP causes issues during deployment.

Unable to deploy a service for Compellent component with same server object and volume names

You cannot deploy a service for Compellent component if the server object is already mapped to the volume. This error occurs because a volume name available in recycle bin is same as the volume that the resource module is trying to create using ASM UI.

You must have unique names for Volumes and Server Objects in the system (even if the volumes and server objects are in different folders) because of the issues caused in Compellent API and UI behavior.

Unable to deploy a service using the template with two EqualLogic CHAP components

Unable to deploy a service using the template with two EqualLogic CHAP components.

In ASM 8.3 release, you cannot create a template with two EqualLogic CHAP components and deploy a service that includes ESXi hosts attached to storage. Currently, ESXi deployments support a single EqualLogic component.

Unable to log in to ASM using active directory using ""

You cannot log in to ASM using Active Directory with the domain name and user name separated by back slash "\".

To log in to ASM using Active Directory, use forward slash "/". For example: <domain>/ <username>.

NOTE: Domain is the name for the Active Directory service you have created in ASM.

Chain booting issue occurs while booting microkernel in a multi-hop DHCP environment

The chain booting error occurs if the DHCP server is configured in a different subnet or network or connected to a different switch.

In such scenarios, the DHCP network is tagged.

To resolve this issue, in switch configuration, modify the native VLAN of server or computer facing ports to PXE VLAN.

Sample native VLAN configuration in Dell PowerConnect switch:

interface Gi1/0/2

spanning-tree portfast

switchport mode general

switchport mode general

switchport general allowed

vlan add 3000

switchport general allowed

vlan add 20,30,40 tagged

exit

In the above example:

- 3000: Indicates Native PXE VLAN
- 20,30,40: Indicates Management or vMotion or ISCSI

In case of production environments with large networks, routers may be configured with IP Helper Addresses to point to a DHCP on another network.

The health status for Compellent storage devices displays as Unknown on the Resources page

Make sure that the Compellent SNMP agent is configured with the same public string that is used in the Compellent credentials, the SNMP agent is started, and enabled on the device.

Scaling down a server that is part of a cluster with HA and DRS disabled does not remove the server from vCenter. The associated virtual machines may also appear in a Disconnected state.

It is recommended that before you scale down a server, you must migrate the VMs to a different host if HA and DRS are not enabled on the cluster.

Firmware update on a server fails with a POST error

Ensure that the **F1/F2 Prompt on Error** option in the BIOS is set to disabled.

Stale Active Directory account entries for HyperV host and cluster can fail HyperV deployments.

A HyperV deployment may fail if stale Active Directory account entries corresponding to a host or a cluster name are used in a deployment. Ensure that you clear the unused and stale entries from Active Directory and then try a deployment.