Active System Manager
Version 8.0 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.

Copyright

2014 - 11

Rev. A00

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.

The new 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, version 8.0.

What is New in this Release

- Infrastructure firmware compliance and updates
- Wizard based chassis, server and IO onboarding with advanced configuration
- 13th generation server support.
- Streamlined installation experience
- FCoE support with Brocade, Dell s5000, and Cisco Nexus
- Resource health monitoring
- Enhanced role-based access control
- Service Lifecycle Improvements including scheduling a service deployment and scaling down a running service

Accessing Online Help

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

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.

Additionally, 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 the ASM.

Go to http://www.dell.com/asmdocs.

- *Dell Active System Manager version 8.0 Release Notes*
- *Dell Active System Manager version 8.0 Quick Installation Guide*
- *Dell Active System Manager version 8.0 Compatibility Matrix Guide*

For more information about best practices, Dell solutions, and service, see Dell Active System Manager page on Dell Techcenter -

http://en.community.dell.com/techcenter/converged-infrastructure/w/wiki/4318.dell-active-system-manager.aspx

Licensing

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

ASM 8.0 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 will receive an e-mail from customer service with the instructions for downloading ASM. The license file is attached to that email.

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

After uploading an initial license, subsequent uploads replace the existing license.

2

Getting started with ASM 8.0

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 indicates that you have completed the step.

NOTE: Standard users do not have the privilege to view the **Getting Standard** page.

The steps include:

- **Step 1: Initial Setup** — Click **Initial Setup** to configure basic settings required before you start using ASM, such as license, virtual appliance time zone, NTP server, DHCP, and proxy server settings. To proceed to Step 2, you must complete the initial setup configuration.

  After initial setup is complete, to edit the NTP, DHCP Server, proxy server, and license information, click **Settings** in the left pane, and then click **Virtual Appliance Management**.
- **Step 2: Define Networks** — Click **Define Networks** to define networks that are currently configured in your environment for resources to access. To define, edit, or delete your existing networks, in the left pane, click **Settings** in the left pane, and then click **Networks**.
- **Step 3: Discover Resources** — Click **Discover Resources** to discover one or more resources (chassis, blade server, switch, storage, and hypervisor management software instances) that you want ASM to manage on your network. Additionally, following information is displayed on the **Disover** pane.
  - **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 to discover the number of resources displayed due to some issues.
- **Step 4: Configure Resources** — Click **Configure Resources** to perform a firmware compliance check on the resources that are discovered and configure the chassis as needed.
- **Step 5: Publish Templates** — Click **Publish Templates** to open the **Templates** page. On the **Templates** page, create a new template or edit a draft default template and publish it. After the templates are published, they are ready to deploy.

NOTE:
To view the left-hand navigation pane options, at least a template must be in the published state.

When the initial setup and discovery step are complete, you can still discover resources, create or edit templates, and publish templates from the left pane.

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, click **Settings** in the left pane, and then click **Getting Started**.

Related Links

Discovery overview
Initial setup

3

Initial setup

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

Before you begin, gather the following information:

- The local network share that contains 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) servers.
- 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 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, add 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
Configure proxy settings
Configure DHCP settings

Uploading license

If you are using ASM for the first time, you must upload the license file through the **Initial Setup** wizard. To upload a subsequent license, click **Settings** in the left pane, and then click **Virtual Appliance Management**. In 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 it 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. Click **Save and Continue** to activate the license.

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 host ASM and configure Network Time Protocol (NTP) servers used for time synchronization.

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

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 **Settings** in the left pane, and then click **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

Configure 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 through 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. Click **Test Proxy Connection** to test the connection to the proxy server.
6. Click **Save and Continue**.

After the initial setup is complete, to change the proxy settings, in the left pane, click **Settings** in the left pane, and then click **Virtual Appliance Management**. 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 if you want to set 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 server 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 will be 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 short duration. That is for 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 will be 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 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 navigation bar.

4

Dashboard

The **Dashboard** displays the following information:

NOTE: Standard users are allowed only to view the details of the services that they have created or for the services they have permission.

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

    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 are listed at the bottom of the graphical display:

    * State icons. The number next to the icons indicate the number of services that are in a particular state.
    * Service name. Click to view the 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**
- Under **Server Overview → Server Health**, a pie chart displays the total number of servers available across all the server pools and their state.

  The state of the servers are categorized based on the following state:

  – **Healthy** (green band on the graphic): Indicates that there is no issue with the servers and working as expected.
  – **Critical** (red band on the graphic): Indicates critical problems exist with one or more components in the server. These issues should be fixed immediately.
  – **Warning** (yellow band on the graphic): Indicates that the servers are in a state that requires 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 is Services**, a pie chart displays the total number of servers utilized in services and the available servers that can be used in percentage.

  – **Servers In Use** (blue band on the pie chart) — Indicates the percentage of servers that are in use. To view the number of servers used, move the mouse pointer over the band.
  – **Servers Available** (gray band on the graphic) — Indicates the percentage of servers that are available for deployment. To view the number of servers that are available, move the mouse 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 total storage capacity utilized and available in percentage.

  – **Storage Used** (blue band on the graphic) — Indicates total used storage disk space in percentage. To view the percentage of used storage disk space, move the mouse pointer over the band.
  – **Storage Available** (gray band on the graphic) — Indicates total available storage space in percentage. To view the percentage of available storage space, move the mouse 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 of the following events occur:

  – The number of resources managed by ASM exceeds the valid license count.

  - The trial license expires.
- **Deploy Service from Recent Templates** — Enables you to view the most recent published templates and use it for deployment. Click **View All** to view all the templates.

  NOTE: Standard users are allowed only to view the recent templates that they have created.
- **Recent Activity —** Lists the most recent user and system initiated activities. Click **View All** to view all the activities in the **Logs** page.

  Additionally, following information is displayed on the **Disover** pane.

  - **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.

On this page, you can:

- Click the service name to view the details information about the service. For more information, see Viewing Service Details.
- View the most recent published templates and use it for service deployment.

Related Links

Viewing service details
Deploy service
Service states

Service states

State	Icon	Description
Error		Indicates service deployed is failed due to some issues.
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.
In Progress		Indicates service deployment is in progress.
Deployed		Indicates service deployed is completed successfully.

Related Links

Dashboard

5

Services

A service is a deployment of a published template.

NOTE: Standard users are allowed to view only the services that they have created or for which they have permissions.

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

- **Error Services** — Indicates the services for which the deployment process is incomplete due to errors.
- **Deployed Services** — Indicates the services that are deployed successfully.
- **In Progress Services** — Indicates the services for which deployment is in progress.
- **Warning Services** — Indicates that the one or more resources in a service are in a state that requires corrective action.

To switch between Graphical and Tabular view, click the Graphic icon or Table icon next to the **View As** option on the top of the **Services** page.

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**
- **Error**
- **Deployed**
- **In progress**
- **Warning**

In the Graphical view, each graphics represents a service and has the name 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 service for 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 about the service 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

From the **Service** page, you can:

- Click **Deploy New Service** to deploy new service.

  NOTE: Standard users are allowed to deploy services that they have created or for which they have permissions.
- Click **View Details** in the right pane 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 service details to **.csv** file.

  NOTE: Standard users are allowed only to export the details of the services that they have created or for which they have granted permission.

Related Links

Viewing service details
Deploy service

Deploy 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. In the left pane, click **Services**.

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

   The **Deploy Service** wizard is displayed.
3. In the **Service Information** page, perform the following steps, and click **Next**.
   a. From the **Select 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 running on the servers that are in 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 could update the firmware level on servers for this service. Firmware on shared devices will still be maintained by the global default firmware repository.

d. 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 **All Standard Users** option
- To grant access only to specific Standard users, 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 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. In the **Deployment Settings** page, configure the require settings, and click **Next**. Additionally, in the **Deploy Setting** page, click **View All Details** to view the details of the components that are part of the service
5. 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.

Viewing service details

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

To switch between Topology and Tabular view, click the topology icon or graphic icon next to **View As** option on top of the **<Service Name> Details** page.

- 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 indicate the following:

  – The red component icon indicates the service is not deployed on a particular component due to some issues.
  – The blue component icon indicates the service is successfully deployed on the components.
  – The light blue component icon indicates the service deployment is in progress.
  – The yellow icon indicates 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
- In the Tabular view, under **Service Resources**, the following information is displayed based on the resource types in the service.
  - Under **Applications**, you can view the following information about the application deployed on the virtual machines:
    * **Name**
    * **IP Address**
    * **Asset/Service Tag**
  - 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**
    * **Manufacturer**
    * **Model**
  - Under **Physical Servers**, you can view the following information about the servers that are part of a service

    :
    * **IP Address**
    * **Hypervisor IP Address**
    * **Asset/Service Tag**
    * **Manufacturer**
    * **Model**
  - 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**
    * **Manufacturer**
    * **Model**
- Under **Service Information**, you can view the following information:
  - Name of the service

– **State** — Displays one of the following state based on the deployment status of a service.

Service State	Icon	Description
In Progress		Indicates service deployment is in progress.
Error		Indicates service deployment is failed due to some issues.
Successful		Indicates service deployment is completed successfully.
Warning		Indicates that the one of more resource 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.

– **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.

– **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**, you can:

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

Under **Resource Actions**, you can:

- From the **Add Resources** drop-down list, select the type of the resources that you want to add to the service.
- 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)**.
- Click **Delete Resources** to delete resources from a service.

Under **Firmware Actions**, click **View Firmware Compliance Report** link to view the firmware compliance report.

In the **Recent Activity** section, click **View Components** or **View Logs** to either view the deployment state of the resources or view the log entries.

Related Links

Deploy service
Exporting service details
Exporting service details
Updating firmware
Retry failed service
Adding components to existing service deployments
Deleting service
Deleting resources from service
Migrating servers

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.
- Error — 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. In the left pane, click **Services**.
2. On the **Services** page, click the service, and in the right pane click **View Details**.
3. On the **<service name> Details** page, in the right pane, next to **Service Information** section title, 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 running on the servers that are part of the service, select **Manage Server Firmware** check box, and from the **Use Firmware Repository** drop-down list, select a firmware repository.

    NOTE: Changing the firmware repository could 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.

Deleting service

To delete a service, perform the following steps:

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

1. In the left pane, click **Services**.
2. On the **Services** page, click a service, and then in the right pane, click **View Details**.
3. On the **<Service Name> Details** page, under **Service Actions** in the right pane, click **Delete**.
4. In the **Delete Service** dialog box, perform the following steps:

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

   a. Select **Return Servers(s) to Resource Pool** check box to return the IP/IQNs assigned to the servers that were a part of the service and return 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.
   b. Select **Delete VM(s)** check box to delete the virtual machines created on the clusters.
   c. Select **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.
   d. Select **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. In the **Services** page, click **Export to File** in the right pane.
2. Open or save the file.

Retry failed 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. In the left pane, click **Services**.

The **Services** page is displayed.

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

View Service Deployment Settings

The **Service Deployment Settings** page displays the settings configured on the resources in a service for deployment.

- 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, in order 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 prerequisites

- 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 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, additional servers can be migrated. During migration, ASM will try 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. In 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.

Adding components to existing service deployments

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 cannot add a component of a particular type if the component type is not a part of the service reference template.

NOTE: You cannot add components to a service for which deployment is in progress or to a failed service deployment.

To add components to a service:

1. In the left pane, click **Services**.
   The **Services** page is displayed.
2. Select a service and click **View Details** in the right pane.
   The **<Service Name> 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** — to add one or more storage components to the service.

Related Links

Adding storage to existing service
Adding servers to existing service
Adding Virtual Machines to existing service
Adding clusters to existing service
Adding applications to existing service

Adding applications to existing service

To add applications to an existing service:

1. On the **Add Application(s)** page, add the applications to the existing service in one of the following ways:
   - If you want to clone an existing application settings to the applications 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 an application that is part of the service.
     2. In the **# of Instances** box, enter the number of application instances that you want to add to the service. Click **Continue**.
     3. In the **Component Name** box, enter the name for the corresponding applications.
   - If you want to add new application, next to **New Component Settings**, click **New**, and perform the following steps:
     1. From the **Select a Component** drop-down list, select one of the following cluster types:
        - **mssql**
        - **citrix_xd7**
        - **linux_postinstall**
        - **mssql2012**
        - **windows_postinstall**
     2. Under **Associated Resources**, to associate the newly added application 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 to component type settings, see Component Types.
2. Click **Save**.

Adding clusters to existing service

To add clusters to an existing service:

1. On the **Add Cluster(s)** page, add the clusters to the existing service in one of the following ways:
   - If you want to clone an existing cluster configuration to the clusters 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 cluster to clone.
     2. In the **# of Instances** box, enter the number of cluster instances that you want to add to the service. Click **Continue**.
     3. In the **Component Name** box, enter the cluster name for the corresponding clusters.
   - If you want to add new cluster component, next to **New Component Settings**, click **New**, and perform the following steps:

1. From the **Select a Component** drop-down list, select one of the following cluster types:
   - **VMWare Cluster**
   - **Hyper-V Cluster**
2. Under **Associated Resources**, to associate the newly added cluster 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 to component type settings, see Component Types.

2. Click **Save**.

Adding Virtual Machines to existing service

To add virtual machines to an existing service:

1. On the **Add VM(s)** page, add the virtual machines to the service in one of the following ways:
   - If you want to clone an virtual machine configuration to the virtual machines 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 virtual machine component.
     2. In the **# of Instances** box, enter the number of virtual machine instances that you want to add to the service. Click **Continue**.
     3. In the **Component Name** box, enter the virtual machine name for the corresponding components.
     4. In the **Host Name** box, enter the host name of the virtual machines.
   - If you want to add new virtual machine instance, click **New**, and perform the following steps:
     1. From the **Select a Component** drop-down list, select on of the following:
        - **vCenter Virtual Machine**
        - **Clone vCenter Virtual Machine**
        - **Clone Hyper-V Virtual Machine**
     2. Under **Associated Resources**, to associate the newly added virtual machine 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 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.
- 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 “Available” to “Reserved”. 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 “Error”.

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 in one of the following ways:
   - If you want to clone an existing storage configuration to the storage 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 storage component.
     2. In the **# of Instances** box, enter the number of storage instances that you want to add to the service. Click **Continue**.
     3. In the **Component Name** box, enter the storage name for the corresponding components.

4. In the **Storage Volume** box, enter the volume name in the storage.

- 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 one of the following storage components:

     – **Compellent**
     – **EqualLogic**
     – **NetApp**

  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**.

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 will be 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 specifically categorized as:

- Application
- Virtual Machine
- Cluster
- Server
- Storage

NOTE: The Switch component cannot be configured in ASM currently.

The Templates page allows you to access default Dell templates or create new 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 in order 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.

Related Links

Manage templates
Sample templates
Cloning template
Deleting template
Creating template
Editing template

Building and publishing template
Importing template
About roles

Manage 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 the particular components are part of the template. The component icons in gray indicate 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 new template.
- Click the template and perform the following actions on 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 Template** to use the properties of this template and create a new template.

Related Links

Sample templates
Creating template
Editing template
Deleting template
Cloning template
Importing template
Deploy 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 details about the components settings, see Component Types

Related Links

Component types

Creating template

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

To create a new 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.
   In case of **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 new category, select **Create New Category** from the list.
6. Enter **Template Description**. (Optional).
7. If you want to update the firmware 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, select a firmware repository.

NOTE: Changing the firmware repository could 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 users 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
Sample templates

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 **Template Name** box, modify the template name as needed.
4. From the **Template Category** drop-down list, select a template category. To create a new category, select **Create New Category** from the list.
5. In the **Template Description** box, enter the description for the template..
6. If you want to update the firmware 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, select a firmware repository.

   NOTE: Changing the firmware repository could update the firmware level on servers for this service. Firmware on shared devices will still be maintained by the global default firmware repository.
7. 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, 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 users to the list displayed.

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.

8. 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, 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 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
Deploy service
Sample templates

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, click **Create Template**, or in the right pane, click **Edit** to edit an existing template.
3. On the Template Builder page, 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**.

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:

- Click **Edit** next to the Template Information section title, to edit the template information.
- 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 the permission is granted to one or more Standard users.
  - Under **Actions**, you can:
    * Click **Publish Template** to publish the template. Once it is published it can be deployed as a service.
    * Click **Delete Template** to delete the template.
    * Click **View All Settings** to view all the resources that are in the template and their properties.
    * Click **Import Template** to import the configuration from an existing 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 details 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 **OK** when a warning message is displayed.

Related Links

Sample templates

Cloning template

The **Clone** option allows you to copy an existing template into a new template. A cloned template will contain 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. Click **Templates**.
2. Select a template, and click **Clone**.

   You can also clone an existing template while creating a new template. For more details, refer to the **Create a Template** topic.
3. Enter a **Template Name** and **Template Description** (Optional), and click **Save**.

Deploy 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. In the left pane, click **Services**.

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

   The **Deploy Service** wizard is displayed.
3. In the **Service Information** page, perform the following steps, and click **Next**.

   a. From the **Select 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 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 could update the firmware level on servers for this service. Firmware on shared devices will still be maintained by the global default firmware repository.

   d. 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.
4. In the **Deployment Settings** page, configure the require settings, and click **Next**. Additionally, in the **Deploy Setting** page, click **View All Details** to view the details of the components that are part of the service.

5. 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 existing service deployments
Retry failed service
Deleting service

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 is to turn off the host. For server, additional cleanup is required after turning off the server. For storage provisioned by ASM, the default behavior when a service is deleted is to retain the storage volume available to make sure 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 required, 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 required, 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: Currently, ASM does not support Switch configuration.

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
Server
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 Chap
- NetApp

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**
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

NOTE: Currently, you can add only one instance of Compellent storage type while building a template. However, you can add multiple EqualLogic storage components in the template.

Storage settings

Field Name	Description
EqualLogic Chap Storage Settings	
Target EqualLogic Device	Specifies the EqualLogic storage device where the volume is created.
Storage Volume	Select the volume in Equallogic. To create a new 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. 100m, 1g)	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 or not a thin provisioning sends an initiator warning when passing the in-use warning threshold.
Thin Warning Hard Threshold %	Specifies whether or not a thin provisioning allows the volume to remain online after reaching the max-growth threshold.
Multi-host access of volume	This parameter enables or disables multi-host 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.

Field Name	Description
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**.
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 Device	Specifies the compellent storage device where the volume is created.
Storage Volume	Specifies the name of the volume that is to be created or destroyed.
Storage Size e.g 100g	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 Type	Specifies the operating system type, which is set in the compellent server object of the compellent storage center.

Field Name	Description
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 *FibreChannel* and *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 already exists. The possible values are *true* or *false*.
Map Read Only	Specifies whether or not 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 will be created.
Storage Volume *	Select the volume name on the NetApp array. To create a new 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 100GB *	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.
The space reservation mode	Specifies the type of volume that guarantee the new volume will use. 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.

Field Name	Description
Persistent	• In Data ONTAP 7-Mode, the persistent is enabled by default. If it is enabled, modifies 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.

Server

To provision a bare metal server, add a server component in the template builder.

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

1. In the **Server Component** dialog box, from the **Select a Component** drop-down list, select a server component.
2. In the **# of Instances,** box, enter the number of the server instances that you want to add.
3. Under **Related Components**, select the components that you want to map with the server components. For more information about valid component combinations that can be mapped together in a template, see Component Combinations in Templates
4. Click **Continue**.
5. To import an existing server configuration and use it for the server component settings, click **Import from Reference Server**. On the **Select Reference Server** page, select the server from which you want to import the settings, and click **Select**.
6. To import configuration from a server that is part of an existing templates, click **Import from Existing Template**. On the **Select Component** page, select the server under a template, and click **Select**.
7. Specify the settings to be configured on the server components.

   For more information about the server settings, see Server Settings
8. Under **Network Settings**, perform the following settings:

   a. In the **Identity Pool**box, enter the virtual identity pool from which virtual identities (MAC address and WWPN/WWNN) will be selected for boot from SAN deployment.

   b. Specify the networks that you want configure on the servers.

      - For configuring interface on the Rack Servers, see Configuring Interface on RackServers
      - For configuring interface on the Blade Servers, see Configuring Interface on Blade Servers
9. Click **Add**.

Server settings

Target Boot Device	Description
Hardware Settings	
Target Boot Device	Specifies the target boot device (for example: Local Hard Drive or SD card).
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 Core Processors	Specifies the number of enabled cores per processor.
Processor Virtualization Technology	If this is enabled, the additional hardware capabilities provided by virtualization technology are enabled.
Logical Processors	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.
Memory Node Interleaving	If the system is configured with matching memory, enables memory node interleaving. If disabled the system supports non-uniform memory architecture memory configurations.
Execute Disable	Enables or disable execute disable memory protection
Server Pool	Specifies the pool from which servers are selected for the deployment.
OS Settings	
OS Image Type	Refers to the operating system types that are available for deployment, such as Red Hat, Linux, Windows, and Hyper-V. The image type corresponds to the installers that are shipped with ASM for installing a particular type of operating system. For example, you can install Red Hat 6.1, 6.2, 6.3 images and install them all with the Red Hat image type. NOTE: Based on the value selected from the **OS Image Type** drop-down list, the fields related to that OS type are displayed.
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.
Administrator password	Enter the administrator password that set on the installed OS.
Confirm administrator password	Enter to confirm the administrator password.
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.

Target Boot Device	Description
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.
Custom Installation OS Script	Refers to ASM maintained kickstart scripts or **unattend.xml** customer specific scripts to be used as a part of unattend OS install.

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

Configuring interface on rack servers

To add a server interface:

1. In the **Server Component** dialog box, select **Rack Server** option under **Targeted Server Type**:
2. For Rack Servers, under Interfaces, click Add New Interface.
3. From the NIC Type, select the NIC type:
   - 2 Port
   - 4 Port
4. Select the **Used for FC** check box, if you want to use the NIC for Fibre Channel.
5. Under specific ports, if you want to partition the port, select the **Do you want to partition?** check box.
6. Enter the following information for each ports or partitions:
   a. Select the vLAN Networks to use for data transmission
   b. Enter the Minimum Bandwidth and maximum bandwidth in percentage.
7. Repeat the steps 4 through 6 for each port.
8. After configuring interfaces, you can configure NIC Teams.
9. Click **Add**.

Configuring interface on blade servers

1. In the **Server Component** dialog box, under **Fabric Configuration**, select **Blade Server**.
2. To enable the fabrics, select the corresponding check boxes next to **Fabric A**, **Fabric B**, and **Fabric C**.
3. Under **Used for FC**, select the check boxes next to **Fabric B** and **Fabric C** if you want to enable the fabrics for Fibre Channel traffic.
4. From the **NIC Type**, select one of following NIC types:
   - **2 Port**
   - **4 Port**
5. Under **<Port number>**, if you want to partition the port, select the **Do you want to partition?** check box.
6. Perform the following steps for each port and partitions:
   a. In the **Network (vLAN)** column, select the network that you want to configure on the port and partition.
   b. Enter the **Minimum Bandwidth** and **Maximum Bandwidth** in percentage.
7. Repeat the steps 4 through 6 for each port and partition.
8. Click **Add**.

Importing from reference server

The **Importing From Reference Server** feature enables you to import an existing server configuration and use it for the new server component settings. You can edit the settings after importing the configuration.

To import a server configuration, perform the following steps:

1. On the **Server Component Settings** page, click **Import from Reference Server**.
2. In the **Select Reference Server** dialog box, click the server to import the configuration.
3. Click **Select**.

Importing from existing template

The Importing From Existing Template feature enables you to import configuration from a server that is part of an existing templates. You can edit the settings after importing the configuration.

To import a configuration from a server that is part of a template, perform the following steps:

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**.

Cluster

In ASM, adding a Cluster component to a template refers to creating a cluster inside a VMware vCenter and SCVMM.

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 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

Field Name	Description
Cluster Settings (Target vCenter)	
Target Hypervisor	Specifies the target VMware vCenter.
Data Center Name	Specifies the name of the data center to be created in VMware vCenter. The keyword cluster is not required.
New datacenter name	Enables to specify a new data center.
Cluster Name	Specifies the name of the cluster to be created in the Data Center.
New cluster name	Enables you to specify a new cluster.
Cluster HA	Enables or disables highly available cluster.
Cluster DRS	Enables or disables distributed resource scheduler.
Cluster Settings (Target Hyper-V)	
Hypervisor Management Software	Specifies the target SCVMM.
Host Group	Specifies the host group that you want to target.
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 Virtual Machine on the template builder page, perform the following actions:

After selecting **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

Virtual Machine Settings (Clone vCenter Virtual Machine)	
Field Name	**Description**
vCenter Virtual Machine	
Virtual Machine OS Settings	
Administrator password	Specifiy OS administrator password that is set on the installed OS.
Confirm administrator password	Enter the password to confirm the administrator password.
OS Image	Specifies the target repository where the OS image install files are located. The default repositories are ESXi. The additional repositories will be shown if the user created them on the ASM appliance.
OS Image Type	Refers to the operating system types (for example: Red Hat, Linux, Windows and so on.) that are available for deployment. The image type corresponds to the razor “installers” that are shipped with razor and assist razor in installing a particular type of operating system. For example, you can install Red Hat 6.1, 6.2, 6.3 images and install them all with the Red Hat image type.
Custom Installation OS script	Refers to ASM maintained kickstart scripts or unattend.xml customer specific scripts to be used as a part of unattend OS install.

Virtual Machine Settings (Clone vCenter Virtual Machine)	
Field Name	**Description**
Virtual Machine Settings	
Number of CPUs	Refers to the number of CPUs specified while configuring a Virtual Machine.
Virtual Disk Size (GB)	Specifies the size to allocate for virtual machine hard disk.
Memory in MB	Refers to the memory in GB specified while configuring a Virtual Machine.
Networks	Specifies the networks that will be associated with the virtual machine. Any networks must be available on the virtualization host for the VM.
Virtual Machine Settings (Clone Hyper-V Virtual Machine)	
Number of CPUs	Refers to the number of CPUs specified while configuring a Virtual Machine.
Virtual Disk Size (GB)	Specifies the size to allocate for virtual machine hard disk.
Memory in MB	Refers to the memory in GB specified while configuring a Virtual Machine.
Networks	Specifies the virtual machine networks to be connected to the virtual machine.
Name	Specifies the name of the virtual machine.
Source	Specifies the name of the source template.
Source Datacenter	Specifies the VMware data center where the source template or virtual machine resides.
Virtual Machine Settings (Clone Hyper-V Virtual Machine)	
Description	Refers to 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 will be deployed
Networks	Specifies the ASM networks, which will be connected to the virtual machine clone.
Block Dynamic Optimization	If it is `True`, the block dynamic optimization will be 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

Virtual Machine Settings (Clone vCenter Virtual Machine)	
Field Name	**Description**
Start Action	Selects the action to perform automatically when the virtualization server starts.
Start Action	Selects the action to perform when the virtualization server stops.

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.

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 selection, the page displays the application properties for you to configure properties.
5. Under **Application Settings**, specify the application properties.

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

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 just 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, DREPLAY_CTLR,`

Field Name	Description	Default and Possible Values
		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/ XenDesktop Setup"

Field Name	Description	Default and Possible Values
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`
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`
yum_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**

Field Name	Description	Default and Possible Values
Upload Recurse	Determines whether or not 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 a number of 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

Valid Component Combinations in Templates (X's in columns indicate components that can be used together in a template)											
Application					X		X			X	
Virtual Machine				X	X				X	X	X
Cluster			X	X	X			X	X	X	X
Server		X	X	X	X	X	X				X
Storage	X	X	X	X	X						

Sample templates

ASM ships with several templates to guide you to develop a template. It is recommended not to alter the default templates, and clone a version, which contains the settings unique to your environment. After you clone the template, you should make minor modifications to make sure the template deploys in your environment.

Related Links

Template – deploy Citrix XenDesktop for 500 users
Template – deploy operating system to hard drive

Template – deploy physical server and virtual machine
Template – deploy virtual machines to cluster
Template – install ESXi to SD card with Fibre Channel storage
Template – install ESXi to SD card with iSCSI storage
Template – deploy Hyper-V host with iSCSI storage
Template – deploy Hyper-V cluster with iSCSI storage
Template – deploy Hyper-V cluster with Fibre Channel storage to SCVMM
Template – deploy VMware cluster with NetApp storage
Template – boot from Fibre Channel SAN
Template – boot from iSCSI SAN
Template – deploy virtual machine template clone on Hyper-V cluster
Template – deploy virtual machine template clone on VMware cluster

Template – deploy Citrix XenDesktop for 500 users

This template provides virtual infrastructure (storage, hosts and cluster) for 500 desktop users.

1. In the **Templates** page, select the **Deploy Citrix XenDesktop for 500 Users** and then click the **Clone** button.
2. In the **Create Template** dialog box, enter the **Template Name** and **Template Description** for the template.
3. On the Template Builder page, click a storage component, click **Edit** in the box that is displayed, and then configure the following settings in the **Storage Component** dialog box. Repeat this step for each storage components.

    a. In the **Component Name** box, type the component name. (Optional)

    b. Under **Storage Settings**, configure the following:

        1. Enter the unique names for the **Storage Volume Name** and **Storage Pool**. (Optional)
        2. Update the values of **Storage size**, **Thin Provisioning**, **Snapshot Reserve %**, **Thin Min Reserve %**, **Thin growth Warning %**, **Thin growth Maximum %**, **Thin warning on threshold %**, and **Multi-Host access of volume**.
        3. From the **Authentication** drop-down list, select authentication type as **CHAP**.
        4. Update the **Chap username** and **Chap secret** text boxes for volume access.
4. On the Template Builder page, click the server component, click **Edit** in the box that is displayed, and then configure the following settings in the **Server Component** dialog box. Repeat this step for each server components.

    a. In the **Component Name** text box, type the component name. (Optional)

    b. Under **Hardware Settings** section, configure the following settings:

        1. Retain the value of **Target Boot Device** as default value of SD Card.
        2. From the **Server Pool** drop-down list, select the server pool that contains a target server.

    c. Under **OS Settings**, configure the following:

        1. To select the administrator password that configures on the deployed OS, in the **Administrator password** text box, type the administrator password. In the **Confirm administrator password** box, type the password again to confirm.

NOTE: It is critical to update the password within this template. The value in the template is masked, but the actual password is not set. If this password is not set, you cannot log in to the deployed server.

2. Retain the ESXi value as default in the **OS Image Type** drop-down list.
3. From the **OS Image** drop-down list, select an OS for a hypervisor (Example: ESXi 5.1 or ESX 5.5) that are configured and to be deployed within your ASM managed environment.

d. Under **Network Settings** section, update the network settings accordingly for the hypervisor that you are deploying and for the configured networks in your environment.

5. On the Template Builder page, click the cluster component, click **Edit** in the box that is displayed, and then configure the following settings in the **Cluster Component** dialog box. Repeat this step for each cluster components.

a. In the **Component Name** text box, type the component name. (Optional)

b. Under **Cluster Settings**, configure the following:

1. From the **Target Hypervisor** drop-down list, select the target vCenter.
2. In the **Data Center Name** and **Cluster Name** text boxes, type their corresponding names.

6. On the Template Builder page, click the virtual machine component, click **Edit** in the box that is displayed, and then configure the following settings in the **Cluster Component** dialog box. Repeat this step for each cluster components.

a. Enter the **Administrator password**.

b. From the **OS Image** drop-down list, select the Windows Image to deploy Windows on the virtual machine.

c. Select the **Workload** check box next to the **Networks** field if you want workload networks to access this VM.

NOTE: Make sure that the same workload network that you have selected was selected for both of the servers in the Template Builder.

7. On the Template Builder page, click the application component, click **Edit** in the box that is displayed, and then configure the following settings in the **Application Component** dialog box. Repeat this step for each application components.

a. In the **Source Location** box, enter the directory location where the Citrix XenDesktop7 ISO was unpacked. You should enter the directory location for each of the application components.

The location for the directory is **//<ASM appliance IP>razor/XenDesktop7/x64/XenDesktop Setup**.

8. To save the settings, click **Save**.
9. To publish the template, click **Publish Template**.

The template is now ready to be deployed.

Template – deploy operating system to hard drive

This template deploys an OS to the local hard disk drive of a bare metal server. A single server component is available in the Template Builder.

1. In the **Templates** page, select the **Deploy OS to Hard Drive** template, and then click **Clone** in the right pane.
2. In the **Create Template** dialog box, enter the **Template Name** and **Template Description**.
3. Click **Save**.

4. In the Template Builder, click the server component, click **Edit** in the dialog box that is displayed, and then configure the following settings in the **Server Component** dialog box.
5. In the **Component Name** box, type the component name. (Optional)
6. Under **Hardware Settings**, perform the following:
   a. From the **Target Boot Device** drop-down list, select the corresponding target boot device.
   b. From the **Server Pool** drop-down list, select the corresponding server pool.
7. Under **OS Settings**, perform the following:
   a. To select the administrator password that you want to configure on the deployed OS, in the **Administrator password** box, type the administrator password.
   b. In the **Confirm administrator password** box, retype the password again to confirm.

      NOTE: It is critical to update the password within this template. The value in the template is masked, but the actual password is not set. If this password is not set, you cannot log in to the deployed server.
   c. From the **OS Image** drop-down list, select an OS image that is configured and to be deployed in your ASM managed environment.
   d. From the **OS Image Type** drop-down list, select an OS image type that corresponds to the type of OS image you have selected.
8. Under **Network Settings**, update the network settings accordingly for the hypervisor that you are deploying and for the configured networks in your environment.
9. To save the settings, click **Save**.
10. To publish the template, click **Publish Template**.

    The template is now ready to be deployed.

Template – deploy physical server and virtual machine

This template deploys two virtual machines to an existing cluster in vCenter.

1. On the **Templates** page, select the **Deploy Physical Server and Virtual Machine**, and then click **Clone** in the right pane.
2. In the **Create Template** dialog box, enter the **Template Name** and **Template Description**.
3. In the Template Builder, click the server component, click **Edit** in the dialog box that is displayed, and then in the **Server Component** dialog box, perform the following configurations:
   a. In the **Component Name** text box, type the component name. (Optional)
   b. Under **Hardware Settings**, from the **Server Pool** drop-down list, select the corresponding server pool.

   NOTE: It is critical to update the password within this template. The value in the template is masked, but the actual password is not set. If this password is not set, you cannot log in to the deployed server.
4. Under **OS Settings**, perform the following:
   a. To select the administrator password that configures on the deployed OS, in the **Administrator password** text box, type the administrator password. In the **Confirm administrator password** box, type the password again to confirm.
   b. From **OS Image Type** drop-down list, select an OS image type that corresponds to the type of OS image you have selected.

c. From **OS Image** drop-down list, select an OS for a hypervisor (Example: ESXi 5.1) which is configured to be deployed within your ASM managed environment.

5. Under **Network Settings** section, update the network settings accordingly for the hypervisor you are deploying and for the configured networks in your environment.
6. In the Template Builder, select the cluster component, click **Edit** in the box that is displayed, and then configure the .following settings in the **Cluster Component** dialog box.
7. In the **Component Name** text box, type the component name. (Optional)
8. Under **Related Components**, select corresponding components. (Optional)
9. Under **Cluster Settings**, perform the following:

   a. From the **Target Hypervisor** drop-down list, select the target vCenter.

   b. In the **Data Center Name** and **Cluster Name** boxes, type the corresponding names.

10. In the Template Builder, select the virtual machine component, click **Edit** in the box that is displayed, and then perform the following configuration in the **Virtual Machine Component** dialog box. Repeat the following steps for each virtual machine in the cluster.

    a. Under **Virtual Machine OS Settings**, perform the following:

       1. In the **Administrator password** text box, type the administrator password and type the password again in the **Confirm administrator password** box to confirm.

          NOTE: It is critical to update the password within this template. The value in the template is masked, but the actual password is not set. If this password is not set, you cannot log in to the deployed server.

       2. From **OS Image** drop-down list, select an OS image that is configured to be deployed in your ASM managed environment.

       3. From **OS Image Type** drop-down list, select an OS image type that corresponds to the type of OS image you have selected.

    b. Under the **Virtual Machine Settings** section, if the defaults values are not required then edit the **Number of CPUs**, **Virtual Disk Size**, and **Memory in MB**.

11. To save the settings, click **Save**.
12. To publish the template, click **Publish Template**.

    The template is now ready to be deployed.

Template – deploy virtual machines to cluster

This template deploys two virtual machines to an existing cluster in vCenter.

1. In the **Templates** page, select the **Deploy VMs to Cluster** template, and then click **Clone** in the right pane.
2. In the **Create Template** dialog box, enter the **Template Name** and **Template Description** for the template.
3. Click **Save**.
4. In the Template Builder, select the cluster component, click **Edit** in the box that is displayed, and then configure the following settings in the **Cluster Component** dialog box.

   a. In the **Component Name** box, type the component name. (Optional)

   b. Under **Cluster Setting**s, configure the following:

1. From the **Target Hypervisor** drop-down list, select the target vCenter.
2. In the **Data Center Name** and **Cluster Name** boxes, type the corresponding names.

5. In the Template Builder, select the virtual machine component, click **Edit** in the box that is displayed, and then configure the following settings in the **Virtual Machine Component** dialog box. Repeat this step for each virtual machine in the cluster.

   a. Under **Virtual Machine OS Settings**, perform the following:

      1. To select the administrator password that configures on the deployed OS, in the **Administrator password** box, type the administrator password. Reenter the password in the **Confirm administrator password** box to confirm.

         NOTE: It is critical to update the password within this template. The value in the template is masked, but the actual password is not set. If this password is not set, you cannot log in to the deployed server.

      2. From **OS Image** drop-down list, select an OS image that is configured to be deployed in your ASM managed environment.
      3. From **OS Image Type** drop-down list, select an OS image type that corresponds to the type of OS image you have selected.

   b. Under **Virtual Machine Settings**, if the defaults values are not required then edit the **Number of CPUs**, **Virtual Disk Size**, and **Memory in MB** for each virtual machine.

6. To save the settings, click **Save**.
7. To publish the template, click **Publish Template**.

   The template is now ready to be deployed.

Template – install ESXi to SD card with Fibre Channel storage

This template deploys a Fibre Channel storage volume, two ESXi hosts, and creates a VMware cluster.

1. In the **Templates** page, select the **Install ESXi to SD card with FC Storage** template, and then click **Clone**.
2. In the **Create Template** dialog box, enter the **Template Name** and **Template Description** for the template.
3. Click **Save**.
4. In the Template Builder, select the storage component, click **Edit** in the box that is displayed, and then configure the following settings in the **Storage Component** dialog box.

   a. In the **Component Name** text box, type the component name. (Optional)

   b. Under **Compellent Storage Settings**, configure the following:

      1. In the **Storage Volume Name** box, type a unique name.
      2. in **Storage Size e.g 100GB** text box, enter storage size.
      3. Do not modify the **Boot Volume** settings.
      4. In the **Volume Folder**, **Volume notes**, **Replay Profile**, **Storage Profile Name**, and **Server Notes** text boxes, type the details. (Optional)
      5. In the **Server Object Name** box, type a server object name.
      6. From the **Operating System Name** drop-down list, select either VMware ESX 5.1 or 5.5.

7. Retain the values of **Port Type**, **Manual**, **Force Map**, **Map Read Only**, and **Single Path Map** as defaults.

5. In the Template Builder, select the server component, click **Edit** in the box that is displayed, and then configure the following settings in the **Server Component** dialog box. Repeat this step for each server component.

   a. In the **Component Name** box, type the component name. (Optional)

   b. Under **Hardware Settings** section, configure the following:

      1. Retain the value of **Target Boot Device** as default value of SD Card.
      2. From the **Server Pool** drop-down list, select corresponding server pool.

   c. Under **OS Settings**, configure the following:

      1. To select the administrator password that configures on the deployed OS, in the **Administrator password** text box, type the administrator password. In the **Confirm administrator password** box, type the password again to confirm.

         NOTE: It is critical to update the password within this template. The value in the template is masked, but the actual password is not set. If this password is not set, you cannot log in to the deployed server.

      2. Retain the value ESXi as default in the **OS Image Type** drop-down list.
      3. From **OS Image** drop-down list, select an OS for a hypervisor (Example: ESXi 5.1 or ESX 5.5) that is configured to be deployed within your ASM managed environment.

   d. Under **Network Settings** section, update the network settings accordingly for the hypervisor you are deploying and for the configured networks in your environment.

6. In the Template Builder, select the cluster component, click **Edit** in the box that is displayed, and configure the following settings in the **Cluster Component** dialog box.

   a. In the **Component Name** box, type the component name. (Optional)

   b. Under **Cluster Settings**, in the **Data Center Name** and **Cluster Name** boxes, type their corresponding names.

7. To save the settings, click **Save**.
8. To publish the template, click **Publish Template**.

   The template is now ready to be deployed.

Template – install ESXi to SD card with iSCSI storage

This template deploys an iSCSI storage volume, two ESXi hosts, and creates a VMware cluster.

1. In the Templates page, select the **Install ESXi to SD Card with iSCSI Storage** template, and click **Edit** in the right pane.
2. In the **Create Template** dialog box, enter the **Template Name** and **Template Description** for the template.
3. Click **Save**.
4. In the Template Builder, select the EqualLogic storage component, click **Edit** in the box that is displayed, and then configure the following settings in the **Storage Component** dialog box.
5. In the **Component Name** box, type the component name. (Optional)
6. Under **EqualLogic Storage Settings**, configure the following:

   a. From the **Target EqualLogic** drop-down list, select your target EqualLogic iSCSI array.

b. In the **Storage Volume Name** text box, type a unique name.

c. In the **Storage Pool**, **Storage Size**, **Thin Provisioning**, **Snapshot Reserve %**, **Thin Min Reserve %**, **Thin growth Warning %**, **Thin growth Maximum %**, **Thin warning on threshold %**, **Multi-Host access of volume** text boxes, update the values.

d. From the **Authentication** drop-down list, select authentication type as **CHAP**.

e. In the **Chap Username** and **Chap Secret** text boxes, type the CHAP user name and CHAP secret for the volume access.

7. In the Template Builder, select the server component, click **Edit** in the dialog box that is displayed, and then configure the following settings in the **Server Component** dialog box. Repeat this step for both the servers.

   a. In the **Component Name** text box, type the component name. (Optional)

   b. Under **Hardware Settings** section, configure the following:

      1. Retain the value of **Target Boot Device** as default value of SD Card.
      2. From the **Server Pool** drop-down list, select corresponding server pool.

   c. Under **OS Settings**, configure the following:

      1. To select the administrator password that configures on the deployed OS, in the **Administrator password** text box, type the administrator password. In the **Confirm administrator password** box , type the password again to confirm.

         NOTE: It is critical to update the password within this template. The value in the template is masked, but the actual password is not set. If this password is not set, you cannot log in to the deployed server.

      2. Retain the ESXi value as default in the **OS Image Type** drop-down list.
      3. From the **OS Image** drop-down list, select an OS for a hypervisor (Example: ESXi 5.1 or ESX 5.5) which is configured to be deployed within your ASM managed environment.

   d. Under **Network Settings** section, update the network settings accordingly for the hypervisor you are deploying and for the configured networks in your environment.

8. In the Template Builder, click a cluster component, and click **Edit** in the box that is displayed, and then configure the following settings in the **Cluster Component** dialog box.

   a. Under **Cluster Settings**, configure the following:

      1. From the **Target Hypervisor** drop-down list, select the target vCenter.
      2. Under **Cluster Settings**, in the **Data Center Name** and **Cluster Name** text boxes, type their corresponding names.

9. To save the settings, click **Save**.
10. To publish the template, click **Publish Template**.

    The template is now ready to be deployed.

Template – deploy Hyper-V host with iSCSI storage

The **Deploy Hyper-V Host with iSCSI Storage** template deploys two iSCSI storage volumes and installs Hyper-V on a physical host.

To deploy Hyper-V host with iSCSI storage using this template, perform the following steps:

1. On the **Templates** page, select the **Deploy Hyper-V Host with iSCSI Storage** template, and click **Clone**.
2. In the **Create Template** dialog box, enter a name and description for the template, and click **Save**.
3. In the **Template Builder**, select a storage component, click **Edit** in the dialog box that is displayed, and then configure the following settings in the **Storage Component** dialog box.

    a. Modify the **Component Name** with a unique name, if required.

    b. Under **EqualLogic Storage Settings**, configure the following:

        1. From the **Target EqualLogic** drop-down list, select the Target EqualLogic iSCSI array.
        2. In the **Storage Volume Name** box, enter a unique name for the storage volume, if required.

            NOTE: Make sure that you enter the storage size for the first volume is large enough to support your Hyper-V host storage. However, the storage size for the second volume can be small because it is configured as a quorum volume if this host will be used for a Hyper-V cluster. The recommended second volume size is 512 MB.

        3. Verify the values for **Storage Pool**, **Thin Provisioning**, **Snapshot Reserve %, Thin Min Reserve %**, **Thin growth Warning %**, **Thin growth Maximum %**, **Thin warning on threshold %**, **Thin warning on hard threshold %**, and **Multi-Host access of volume**.
4. Click **Save**.
5. In the **Template Builder**, select a server component, click **Edit** in the box that is displayed, and then configure the following settings in the **Server Component** dialog box. Repeat this step for each server component.

    a. Modify the server **Component Name** with a unique name, if required.

    b. Retain the default selection of **Local Hard Drive** for **Target Boot Device.**

    c. Select a **Server Pool** that contains a target server from the drop-down list.

    d. Enter the Windows **Product Key** for the Hyper-V server.

    e. Select the **Timezone** and enter the IP address of the **NTP Server** for time synchronization.

    f. Select the **Language** and **Keyboard** inputs if you do not want to retain default values.

    g. Enter the **Domain Name** and **FQ Domain Name** to which you want to add the Hyper-V host.

    h. Enter the **Domain Admin Username** and **Domain Admin Password** to add the Hyper-V host to the domain and enter the password to confirm.

    i. Enter the **Administrator password** that you want to configure on the deployed OS. Reenter the administrator password to confirm.

        NOTE: It is critical to update the password within this template. There is a masked value present in the template, but there is no actual password set. If you do not set this password, you will not be able to log in to the deployed server.

    j. Select the **OS Image** configured for Hyper-V to deploy within your ASM managed environment.

    k. Retain the default selection of **Hyper-V** for **OS Image Type**.

    l. Under **Network Settings**, update the network settings based on the hypervisor that you want to deploy and the networks you have configured in your environment.

    m. Click **Save**.
6. Click **Publish Template**.

This template is now ready to be deployed.

Template – deploy Hyper-V cluster with iSCSI storage

The **Deploy Hyper-V Cluster with iSCSI Storage** template deploys two iSCSI storage volumes and installs Hyper-V on a physical host.

To deploy Hyper-V host with iSCSI storage using this template, perform the following steps:

1. On the **Templates** page, select the **Deploy Hyper-V Cluster with iSCSI Storage** template, and click **Clone**.
2. In the **Create Template** dialog box, enter a name, description, category for the template, and click **Save**.
3. On the **Template Builder** page, click each storage components, click **Edit** in the box that is displayed, and configure the following settings in the **Storage Component** dialog box.
    a. Modify the **Component Name** with a unique name, if required.
    b. Under **Storage Settings**, configure the following:
        1. Select your **Target EqualLogic** iSCSI array.
        2. Enter the **Storage Volume Name** if required.

        NOTE: Make sure that you enter the storage size for the first volume is large enough to support your Hyper-V host storage. However, the storage size for the second volume can be small because it is configured as a quorum volume if this host will be used for a Hyper-V cluster. The recommended second volume size is 512MB.
    c. Verify the values for **Storage Pool**, **Thin Provisioning**, **Snapshot Reserve %, Thin Min Reserve %**, **Thin growth Warning %**, **Thin growth Maximum %**, **Thin warning on threshold %**, **Thin warning on hard threshold %**, and **Multi-Host access of volume**.
    d. Click **Save**.
4. On the **Template Builder** page, click each server components in the swim lane, and configure the following settings for both the servers:
    a. Modify the server **Component Name** with a unique name, if required.
    b. Under **Hardware Settings**, configure the following:
        1. Retain the default selection of **Local Hard Drive** for **Target Boot Device.**
        2. Select a **Server Pool** that contains a target server from the drop-down list.
    c. Under **OS Settings**, configure the following:
        1. Enter the Windows **Product Key** for the Hyper-V server.
        2. Select the **Timezone** and enter the IP address of the **NTP Server** for time synchronization.
        3. Select the **Language** and **Keyboard** inputs if you want to change the default values.
        4. Enter the **Domain Name** and **FQ Domain Name** to which you want to add the Hyper-V host.
        5. Enter the **Domain Admin Username** and **Domain Admin Password** to add the Hyper-V host to the domain. Enter the domain admin password to confirm.
        6. Enter the **Administrator password** that you want to configure the deployed OS. Reenter the administrator password to confirm.

NOTE: It is critical to update the password within this template. There is a masked value present in the template, but there is no actual password set. If you do not set this password, you will not be able to log in to the deployed server.

7. Select the **OS Image** configured for Hyper-V to deploy within your ASM managed environment.
8. Retain the default selection of **Hyper-V** for **OS Image Type**.

d. Under **Network Settings**, update the network settings based on the hypervisor that you want to deploy and the networks you have configured in your environment.

e. Click **Save**.

5. On the **Template Builder** page, click the **Hyper-V** cluster component, click **Edit** in the box that is displayed, and configure the following settings in the **Cluster Component** dialog box.

a. Make sure that you select your target SCVMM hypervisor from the **Target Hypervisor drop-down** list.

b. Select an existing host group from the **Host Group** drop-down list or enter the name of the host group that you want to create in the **New Host Group name** field.

c. Enter the name of the Host Group you want to create or select the name of an existing host group.

d. Modify the **Cluster Name**, if required.

e. Click **Save**.

6. Click **Publish Template**.

This template is now ready to be deployed.

Related Links

Template – deploy Citrix XenDesktop for 500 users
Template – deploy operating system to hard drive
Template – deploy physical server and virtual machine
Template – deploy virtual machines to cluster
Template – install ESXi to SD card with Fibre Channel storage
Template – install ESXi to SD card with iSCSI storage
Template – deploy Hyper-V host with iSCSI storage
Template – deploy Hyper-V cluster with Fibre Channel storage to SCVMM
Template – deploy VMware cluster with NetApp storage
Template – boot from Fibre Channel SAN
Template – boot from iSCSI SAN
Template – deploy virtual machine template clone on Hyper-V cluster
Template – deploy virtual machine template clone on VMware cluster

Template – deploy Hyper-V cluster with Fibre Channel storage to SCVMM

The **Deploy Hyper-V Cluster with Fibre Channel Storage to SCVMM** template deploys two Fibre Channel storage volumes, installs Hyper-V on two physical hosts, and creates a cluster with the Hyper-V hosts.

To deploy Hyper-V Cluster with Fibre Channel Storage to SCVMM using this template, perform the following steps:

1. On the **Templates** page, select the **Deploy Hyper-V Cluster with Fibre Channel Storage to SCVMM** template, and click **Clone** in the right pane.
2. In the **Create Template** dialog box, enter a name, category, and description for the template, and click **Save**.
3. On the **Template Builder** page, click each storage components, click **Edit** on the dialog box that is displayed, and then configure the following settings in the **Storage Component** dialog box:.

    a. Modify the **Component Name** with a unique name, if required.

    b. From the **Target Compellent** drop-down list, select the target compellent array.

    c. Modify the **Storage Volume Name** and **Storage Size**, if desired.

    NOTE: Make sure that you enter the storage size for the first volume is large enough to support your Hyper-V host or cluster storage. However, the storage size for the second volume can be small because it is configured as a quorum volume if this host will be used for a Hyper-V cluster. The recommended second volume size is 512 MB

4. Click **Save**.
5. On the **Template Builder** page, click each server components, click **Edit** in the dialog box that is displayed, and then configure the following settings for servers in the **Server Component** dialog box:

    a. Modify the server **Component Name** with a unique name, as desired.

    b. Retain the default selection of **Local Hard Drive** for **Target Boot Device**.

    c. From the **Server Pool** drop-down list, select the server pool that has the target server.

    d. From the **OS Image** drop-down list, select the image for the Windows 2012 repository that your Hyper-V install will use.

    e. From the **OS Image Version** drop-down list, select the version of Windows 2012 that will be installed.

    f. Edit the **Administrator Password** for the Hyper-V host.

    g. In the **Product Key** box, enter the Windows Product Key for the Hyper-V server.

    h. Select the **Timezone** and enter the IP address of the **NTP Server** for time synchronization.

    i. Select the **Language** and **Keyboard** inputs if you want to change the default values.

    j. Enter the **Domain Name** and **FQ Domain Name** to which you want to add the Hyper-V host.

    k. Enter the **Domain Admin Username** and **Domain Admin Password** to add the Hyper-V host to the domain. Enter the domain admin password again to confirm.

    NOTE: It is critical to update the password within this template. There is a masked value present in the template, but there is no actual password set. If you do not set this password, you will not be able to log in to the deployed server.

    l. Under **Network Settings**, perform the following:

        1. Clear the **Do you want to partition?** check box.

        NOTE: For a Hyper-V deployment, partitions are not required.

        2. Update the network settings based on the hypervisor that you want to deploy and the networks that you have configured in your environment. Select at least one PXE Network,

Hypervisor Management Network, Hypervisor Migration Network, Hypervisor Cluster Private Network, and an optional Public network for virtual machines.

6. Click **Save**.
7. On the **Template Builder** page, click the Hyper-V Cluster component, click **Edit** in the dialog box that is displayed, and then configure the following settings in the **Cluster Component** dialog box:
   a. From the **Hypervisor Management Software** drop-down list, make sure that you select your target SCVMM.
   b. From the **Host Group** drop-down list, select an existing host group, or in the **New host group name** box and enter the name of the host group that you want to create.
   c. From the **Cluster Name** drop-down list, select **New Cluster** and then in the **New cluster name** box, enter an updated name for the cluster that will be created in SCVMM.
8. Click **Save**.
9. Click **Publish Template**.
   This template is now ready to be deployed.

Template – deploy VMware cluster with NetApp storage

The **Deploy VMWare Cluster with NetApp Storage** template deploys a single NetApp storage volume, installs ESXi on two physical hosts, and creates a cluster with the ESXi hosts.

To deploy VMware Cluster with NetaApp Storage using this template, perform the following steps:

1. On the **Templates** page, select the **VMware Cluster with NetApp Storage** template, and click **Clone** in the right pane.
2. In the **Create Template** dialog box, enter a name, category, and description for the template, and click **Save**.
3. On the **Template Builder** page, click each storage components, click **Edit** on the dialog box that is displayed, and then configure the following settings in the **Storage Component** dialog box:.
   a. Modify the **Component Name** with a unique name, as desired.
   b. From the **Target NetApp** drop-down list, select the target NetApp Storage.
   c. Modify the **Storage Volume Name** and **Storage Size**, as desired.
   d. From the **Aggregate Name**, select the aggregate name that is used in your NetApp storage.
   e. From the **NFS Target IP**, select the target NFS IP that will be used.
4. Click **Save**.
5. On the **Template Builder** page, click each server components, click **Edit** in the dialog box that is displayed, and then configure the following settings for servers in the **Server Component** dialog box:
   a. Modify the server **Component Name** with a unique name, as desired.
   b. Retain the default selection of **SD Card** for **Target Boot Device**.
   c. From the **Server Pool** drop-down list, select the server pool that has the target server.
   d. Edit the **Administrator Password** for the ESXi host.

      NOTE: It is critical to update the password within this template. There is a masked value present in the template, but there is no actual password set. If you do not set this password, you will not be able to log in to the deployed server.

   e. In the **Product Key** box, enter the Windows Product Key for the Hyper-V server.

f. Select the **Timezone** and enter the IP address of the **NTP Server** for time synchronization.

g. Select the **Language** and **Keyboard** inputs if you want to change the default values.

h. Enter the **Domain Name** and **FQ Domain Name** to which you want to add the Hyper-V host.

i. Enter the **Domain Admin Username** and **Domain Admin Password** to add the Hyper-V host to the domain. Enter the domain admin password again to confirm.

NOTE: It is critical to update the password within this template. There is a masked value present in the template, but there is no actual password set. If you do not set this password, you will not be able to log in to the deployed server.

j. Under **Network Settings**, perform the following.

1. Select the **Do you want to partition?** check box.

NOTE: For a Hyper-V deployment, partitions are not required.

2. Update the network settings based on the hypervisor that you want to deploy and the networks that you have configured in your environment. Select at least one PXE network, Hypervisor Management network, Hypervisor Migration network, and an optional Public network for virtual machines.

6. Click **Save**.
7. On the **Template Builder** page, click the VMware Cluster component, click **Edit** in the dialog box that is displayed, and then configure the following settings in the **Cluster Component** dialog box:

a. From the **Target Virtual Machine Manager** drop-down list, make sure that you select your target vCenter.

b. From the **Data Center Name** drop-down list, select **Create New Datacenter**, and enter a data center name in the **New datacenter name** box

c. From the **Cluster Name** drop-down list, select **New Cluster** and then in the **New cluster name** box, enter the cluster name.

8. Click **Save**.
9. Click **Publish Template**.

This template is now ready to be deployed.

Template – boot from Fibre Channel SAN

The **Boot from Fibre Channel SAN** template will create a Compellent storage volume and configure a server to connect to this volume as a boot volume. The resulting server will be ready for manual operating system installation.

To deploy boot from Fibre Channel SAN using this template, perform the following steps:

1. On the **Templates** page, select the **Boot from Fibre Channel SAN** template, and click **Clone** in the right pane.
2. In the **Create Template** dialog box, enter a name, category, and description for the template, select the storage and server components, and click **Save**.
3. On the **Template Builder** page, click the storage component, click **Edit** in the dialog box that is displayed, and then configure the following settings in the **Storage Component** dialog box:.

a. Modify the **Component Name** with a unique name, as desired.

b. From the **Target Compellent** drop-down list, select the target compellent array.

c. From the **Storage Volume Name** list, select **Create New Volume**, and in the **New Volume Name**, enter a new unique volume name.

d. From the **Operating System Name**, select the desired operating system. That is, if using Linux, select ESXi.

4. Click **Save**.
5. On the **Template Builder** page, click the server components, click **Edit** in the dialog box that is displayed, and then configure the following settings for the server in the **Server Component** dialog box:

   a. From the **Server Pool** drop-down list, if required, select the server pool to which you want to deploy.

   b. Under **Network Settings**, select **Blade Server** or **Rack Server** to which you want to deploy.

   c. Select the appropriate workload networks.

   NOTE: Only single function (not partitioned) mode is allowed for boot from SAN.

   NOTE: Only a single VLAN per port is allowed, and this network will be configured as untagged on the server facing port of the switch.

6. Click **Save**.
7. Click **Publish Template**.

   This template is now ready to be deployed.

Template – boot from iSCSI SAN

The **Boot from iSCSI SAN** template will create an iSCSI storage volume and configure a server to connect to this volume as a boot volume. The resulting server will be ready for manual operating system installation.

To deploy boot from iSCSI SAN using this template, perform the following steps:

1. On the **Templates** page, select the **Boot From iSCSI SAN** template, and click **Clone** in the right pane.
2. In the **Create Template** dialog box, enter a name, category, and description for the template, select the storage and server components, and click **Save**.
3. On the **Template Builder** page, click the storage component, click **Edit** in the dialog box that is displayed, and then configure the following settings in the **Storage Component** dialog box:.

   a. Modify the **Component Name** with a unique name, as desired.

   b. From the **Target EqualLogic** drop-down list, select your target iSCSI array.

   c. From the **Storage Volume Name** list, select **Create New Volume**, and in the **New Volume Name**, enter a new unique volume name.

4. Click **Save**.
5. On the **Template Builder** page, click the server components, click **Edit** in the dialog box that is displayed, and then configure the following settings for the server in the **Server Component** dialog box:

   a. From the **Server Pool** drop-down list, if required, select the server pool to which you want to deploy.

   b. Under **Network Settings**, select **Blade Server** or **Rack Server** to which you want to deploy.

   c. For the first network interface, ensure that only your iSCSI network is selected.

   d. For other network interfaces, select the appropriate workload networks.

NOTE: Only single function (not partitioned) mode is allowed for boot from SAN.

NOTE: Only a single VLAN per port is allowed, and this network will be configured as untagged on the server facing port of the switch.

6. Click **Save**.
7. Click **Publish Template**.

   This template is now ready to be deployed.

Template – deploy virtual machine template clone on Hyper-V cluster

The **Deploy Virtual Machine Template Clone on Hyper-V Cluster** template will create a virtual machine clone of a Hyper-V virtual machine template in SCVMM.

NOTE: Template cloning will not work if Hyper-V virtual machine template has not been configured according to the *Active System Manage Quick Install Guide*.

To deploy a Hyper-V virtual machine clone using this template, perform the following steps:

1. On the **Templates** page, select the **Deploy Virtual Machine Template Clone on Hyper-V Cluster** template, and click **Clone** in the right pane.
2. In the **Create Template** dialog box, enter a name, category, and description for the template, select the cluster and virtual machine components, and click **Save**.
3. On the **Template Builder** page, click the Hyper-V Cluster component, click **Edit** on the dialog box that is displayed, and then configure the following settings in the **Cluster Component** dialog box:.

   a. From the **Hypervisor Management Software** drop-down list, select the management software of the target hypervisor for the SCVMM instance where the clone will be created.

   b. From the **Host Group** and **Cluster Name** drop-down lists, select the host group and cluster name on which virtual machine clone will be deployed.
4. Click **Save**.
5. On the **Template Builder** page, click the virtual machine component, click **Edit** in the dialog box that is displayed, and then configure the following settings for the virtual machine in the **Virtual Machine Component** dialog box:

   a. Modify the **Component Name**, **Description**, and **Name** of the virtual machine, as desired.

   b. From the **Template** drop-down list, select a valid Hyper-V virtual machine template that has been created according to the *Active System Manager version 6 Quick Install Guide* instructions.

   NOTE: If the template selected has not been properly prepared, the deployment of the Virtual Machine clone will fail.

   c. Under **Network Settings**, select the network to be associated with the virtual machine.

   NOTE: Any network selected must be enabled and available on the SCVMM hosts/clusters where the virtual machine will be deployed.
6. Click **Save**.
7. Click **Publish Template**.

   This template is now ready to be deployed.

Template – deploy virtual machine template clone on VMware cluster

The **Deploy Virtual Machine Template Clone on VMWare Cluster** template will create a virtual machine clone of a VMware virtual machine template or virtual machine in vCenter.

NOTE: Template cloning will not work if vCenter virtual machine template or virtual machine is not configured according to the *Active System Manage Quick Installation Guide*.

To deploy a VMWare virtual machine clone using this template, perform the following steps:

1. On the **Templates** page, select the **Deploy Virtual Machine Template Clone on VMWare Cluster** template, and click **Clone** in the right pane.
2. In the **Create Template** dialog box, enter a name, category, and description for the template, select the cluster and virtual machine components, and click **Save**.
3. On the **Template Builder** page, click the VMWare Cluster component, click **Edit** on the dialog box that is displayed, and then configure the following settings in the **Cluster Component** dialog box:.
   a. From the **Target Virtual Machine Manager** drop-down list, select the target Virtual Machine Manager instance where the clone will be created
   b. From the **Data Center Name** drop-down list, select the data center on which virtual machine will be deployed.
   c. From the **Cluster Name** drop-down list, select the cluster on which virtual machine will be deployed.
4. Click **Save**.
5. On the **Template Builder** page, click the virtual machine component, click **Edit** in the dialog box that is displayed, and then configure the following settings for the virtual machine in the **Virtual Machine Component** dialog box:
   a. Modify the **Component Name** of the virtual machine, as required.
   b. Under **Network Settings**, select the network to be associated with the virtual machine.

      NOTE: Any network selected must be enabled and available on the SCVMM hosts/clusters where the virtual machine will be deployed.
   c. Update the name for the virtual machine clone.
   d. Select the type of clone to be created, if the source is the virtual machine or if the source is a virtual machine template.
   e. From the **Source** drop-down list, select a valid VMWare virtual machine template or virtual machine that has been prepped according to the instruction provided in the *Active System Manager version 6 Quick Installation Guide*.

      NOTE: If the template selected has not been properly prepared, the deployment of the Virtual Machine clone will fail.
   f. Select the datacenter where the source template is located.
6. Click **Save**.
7. Click **Publish Template**.
   This template is now ready to be deployed.

Template – deploy SQL Server 2012

ASM includes a default template that allows you to deploy SQL Server 2012. To configure this template, you must provide a valid Microsoft SQL Server 2012 ISO and then copy the application location to the ASM virtual appliance.

To configure ASM virtual appliance:

1. Log in to ASM virtual appliance as delladmin. The default delladmin credentials are `delladmin`/`delladmin`.
2. You must copy Microsoft SQL Server 2012 ISO to the **/var/lib/razor/repo-store/** directory.
3. Unpack Microsoft SQL Server 2012 ISO into CIFs share on the virtual appliance. To perform this task, run the following commands: **cd /var/lib/razor/repo-store mount -o loop <SQL2012>.iso/mntrsync -a /mnt/ /var/lib/razor/repo-store/ SQL2012umount /mntrm SQL2012.iso**
4. On the ASM home page, in the left pane, click **Templates**, select the **Deploy SQL Server 2012** template, and then click **Clone**.
5. In the **Create Template** dialog box, enter a name, category, and description. Click **Save**.
6. On the **Template Builder** page, click a storage component, click **Edit** in the box that is displayed, and then configure the following settings in the **Storage Component** dialog box. Repeat this step for each storage components.

    a. Under **Storage Settings**, configure the following:

        1. From the **Authentication** drop- down list, select the one of the following authentication types based on your environment: **IQN/IP** or **CHAP**.
        2. If you have selected the authentication type as **CHAP**, enter the **Chap username** and **Chap secret** for the storage volume
        3. If you have selected the authentication type as **IQN/IP**, enter the **Initiator IQN** or **IP address** for the storage volume.

        NOTE: If you do not update these password values, the template will not deploy correctly. There is no value to passwords in the default template even if a masked value appears. CHAP user names and secrets should be the same on both volumes if CHAP authentication is used.

    b. Verify the **Storage Volume Name**.

    c. Click **Save**.
7. On the Template Builder page, click a server component, click **Edit** in the box that is displayed, and then configure the following settings in the **Server Components** dialog box. Repeat this step for each server components.

    a. Under **OS Settings**, enter the **Administrator password**.

    b. Under **Network Settings**, configure the Hypervisor Management Network, Hypervisor vMotion Network, and Workload networks.

    c. Click **Save**.
8. On the Template Builder page, click the cluster component, and configure the following:

    a. Under **Cluster Settings**, from the **Target Hypervisor** drop-down list, select the target vCenter.

    b. Verify if you want to create a new datacenter or cluster inside your vCenter instance.

    c. Click **Save**.
9. On the Template Builder page, click the virtual machine, and configure the following:

    a. Enter the **Administrator password**.

    b. From the **OS Image** drop-down list, select the Windows Image to deploy Windows on the virtual machine.

    c. Verify the **OS Image Version**.

d. Enter the **Product Key** for corresponding **OS Image Version**.

e. Select the **Workload** networks to access this VM.

f. Click **Save**.

10. On the Template Builder page, click one of the application components, click **Edit** in the box that is displayed, and then configure the following settings in the **Application Component** dialog box:

    a. Under **Application Settings**, in the **Media Location** box, enter the directory location where the SQL 2012 ISO was unpacked.

    b. Add appropriate account name and password information as required.

    c. Click **Save**.

11. Click **Publish Template**.

    This template is now ready to be deployed.

Additional template information

This section provides additional details, including prerequisites, 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

Creating template for ESXi cluster deployment
Deploying service on ESXi clusters
Cleaning up ESXi cluster deployments
ESXi cluster deployment perquisites

ESXi cluster deployment perquisites

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

Specification	Prerequisite
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 will query for WWPN values on a QLogic QME or QLE 2662 or 2572 adapter.
Brocade Switch Configuration	• Create fault domain on Brocade switches for Compellent.

Specification	Prerequisite
	• 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 new 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 will be 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 will be 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
Deploy 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.

Related Links

Understanding All Resources tab
Understanding server pools

Understanding All Resources tab

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

- Health state of the resource (Healthy, Critical, Warning, and Unknown).
- State in which the resource exists Available, Deployed, Pending, Error, and so on.

  NOTE: The state column displays the last discovery state of the resources. To manually run the inventory operation on a resource and update ASM with the latest resource details, click a resource, and then click **Run Inventory** in the **Details** pane.
- IP address of the resource. (Click the IP address of a Dell resource to open the Element Manager.)
- Resource ID that uniquely identifies a resource in the form of service tag, host name, or FQDN based on the resource types.
- Manufacturer name. For example, Dell, Cisco, VMware, and so on.
- Resource model. For example, M620, M1000e, PowerEdge VRTX, and so on.
- Resource type. For example, Chassis, Blade Server, EqualLogic Storage Group, VMware vCenter, and so on.
- Firmware status. (Compliant, Non–Compliant, Update Required)

To sort the resource list based on the entries in a column, click the arrow next the column header.

To filter resources based on the resource types, from the **Resource Type** drop-down list, select one of the following resource types:

- **All Resources**
- **Dell Chassis**
- **Servers**

- **Switches**
- **Storage**
- **VM Manager**

To filter resources based on the resource status, from the **Health** drop-down list, select one of the following resource types:

- **All Resources**
- **Healthy**
- **Warning**
- **Critical**
- **Unknown**

From this page, you can:

- Click **Discover** to discover new resources.
- Click **Remove** to remove the resource from ASM.
- Select one or more resources, click **Manage** or **Unmanage** to allow ASM to manage or unmanage the resources.
- Select one or more resources and click **Update Firmware** to update the firmware 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.
  - Click **Run Inventory** to update the resource inventory.
  - Under **Details**, next to **Firmware Status**, click **View Compliance Report** to view the firmware compliance report

Related Links

Discovery overview
Discovering resources
Viewing resource details
Removing resources
Updating resource inventory
Configuring resources or chassis
Viewing firmware compliance report
Updating firmware
Resource operational state
Resource health status
Resource firmware compliance status

Resource health status

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

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.
	**Critical**	Indicates that there is an issue persist 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.

Related Links

Discovery overview
Discovering resources
Viewing resource details
Removing resources
Updating resource inventory
Configuring resources or chassis
Viewing firmware compliance report
Updating firmware
Resource operational state
Resource firmware compliance status

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.

State	Description
Available	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	Resource is reserved by a service prior to a pending deployment.
Unmanaged	Resource is not managed by ASM.

Resource firmware compliance status

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

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 **Apply Server Firmware Updates** page, select one of the following options..
   - **Update Now** — Select this option to update the firmware immediately.

     ASM will apply 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 will stage the firmware update to each server selected until reboot.

     SM will stage 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 will apply 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.

2. Click **Save**.

Viewing firmware compliance report

To view the compliance report of any resource:

1. On the **Resources** page, select a resource to view the firmware compliance report.
2. In the right pane, under **Firmware Status**, click **View Compliance Report**.

   The **<Resource> Firmware Compliance Report** dialog box displays the following information:

   - **Firmware Name** — Lists the firmware components based on the resource and the associated components.
   - **Firmware Version** — Displays the firmware version running on the components.
   - **Firmware Update Version** — Displays the latest firmware version available for update.
   - **Last Update** — Displays the date and time of the last successful firmware update.

Related Links

Discovery overview
Discovering resources
Viewing resource details
Removing resources
Updating resource inventory
Configuring resources or chassis
Updating firmware
Resource operational state
Resource health status
Resource firmware compliance status

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**.
- In the left pane, click **Resources**. On the **Resources** page, click **Discover** in the **All Resources** tab.

Related Links

Discovering resources

Discovering resources

NOTE: Only the user with Administrator role can discover the resource.

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 Dell resources (chassis, servers, and I/O modules), use the default root-level user name *root*, and password *calvin* for discovery. However, the default root-level credentials are not supported for Dell Compellent Storage Center and Dell EqualLogic Storage.

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. Select the resource type.
   b. Type the IP address range of the resources that you want to discover.
   c. To manage or unmanage the resources that you discover, select **Managed** or **Unmanaged**.
   d. Select or create a new credential to discover resource types.
3. To discover multiple resources with different IP address ranges, repeat the step 2, and then click **Next**.

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

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

Adding IP address range and credentials
Collecting the resource inventory
Adding IP Address and Credentials to Chassis

Adding IP address range and credentials

1. On the **Identify Resources** page, click **Add Resource Type**, and perform the following steps:
   a. From the **Resource Type** drop-down list, select one of the following resource types:
      - **All**
      - **Server**

- **Storage**
- **Switch**
- **vCenter**
- **SCVMM**
- **Chassis**

b. Enter the **Starting IP Address** and **Ending IP Address** range of the resources of same type to discover.

NOTE: You need to use management IP address to discover the NetApp storage resources.

c. From the **Manage in ASM** drop-down list, select one of the following options:

- **Managed** — Select this option if you want manage the resources in ASM.
- **Unmanaged** — Select this option if you do not want to manage the resources in ASM.

d. From the **Credentials** drop-down list, select an existing credential that includes the user name and password to access the resource type, or click the Plus icon to create a new credentials.

NOTE: For Dell resources (chassis, servers, and I/O modules), use the default root-level user name *root*, and password *calvin* for discovery. However, the default root-level credentials are not supported for Dell Compellent Storage Center and Dell EqualLogic Storage.

2. To discover a different resource type and resources of same type with different credentials, repeat the step 1.
3. Click **Next** to discover and collect the inventory data from the resources.

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** — Active System Manager 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** — Active System Manager 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 new 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 new 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. Click **Finish** to collect the inventory data from the resources.

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

Configuring resources or chassis

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

- Remove one or more resource 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.

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 additional 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 uplinks ports on the MXL switches with in 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
Configuring uplink ports
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 resource that you do not want to be in ASM environment, and click **Remove Resource from ASM**.

When you 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 new firmware repositories.
- Click **Remove** to remove a repository
- Click **View Details** to view the firmware bundles that are available in the firmware repository.
- Select a repository from the list and click **Set as Default** to set the repository as default firmware repository.

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** → **Resources** tab, the **Firmware Compliance** state of the resources that is not compliant is displayed as either **Update Required** or **Non-Compliant** .

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 the one or more chassis that you want to configure.
3. Under **Global Settings**, in the **Users** section, configure additional 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 will receive email alerts.

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

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

   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. Click **Next** to configure the unique chassis settings.

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(s), 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.
   - **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 servers:

- **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. Click **Next** to configure the IO modules within the chassis.

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 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. Click **Finish** to configure the uplink ports.

Configuring uplink ports

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

NOTE: ASM supports configuration of uplinks only on MXL Switches. For the IOAs that are not supported, you cannot configure uplinks on the ports.

From this page, you can:

- Define the uplinks. see Defining Uplinks.
- 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 Configuring Uplink Ports on All Chassis Independently

Related Links

Defining uplinks
Configuring uplink ports on all chassis the same
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**.

Configuring uplink ports on all chassis independently

1. On the **Uplink Port 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. In the Configure Uplinks area, expand the chassis section, and 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.
6. Click **Next**.

Configuring uplink ports on all chassis the same

1. On the **Uplink Port Configuration** page, select the **Configure Uplinks** check box.
2. Select **Configure Uplink Ports on All Chassis the Same** 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.
6. Click **Next**.

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 are displayed as **Updating** until the configuration is complete.
2. If you want 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 **Role** 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.

Removing resources

NOTE: On the user with Administrator role can remove the resource from ASM.

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

1. In the left pane, 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 any 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.

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. In the left pane, 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**.

   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.

Managing and unmanaging resources

You can manage or unmanage a resource that is discovered in ASM.

NOTE: Only the user with Administrator role can change resource state to manage or manage in ASM.

1. In the left, select **Resources**.
2. On the **Resources** page, perform the following actions:
   - Select the resources that you want to manage and click **Manage**.
   - Select the resources that you do not want ASM to manage, click **Unmanage**.

Viewing resource details

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

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

1. In the left pane, click **Resources**.
2. In the **Resources** page, select the **All Resources** tab.
3. From the list of resources, click a resource for which you want to view the details.

The **Details** pane in the right displays the basic information about the resources based on the resource type selected.
From this **Details** pane, you can:

- View detailed information about the resources and associated components.

  NOTE: In ASM 8.0 release, the detailed information can be viewed only for Dell Resources.
- Update resource inventory data.

Related Links

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

Viewing chassis details

1. In the left pane, 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**
   - **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. In the left pane, 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 in the right displays the basic information about the blade servers, such as Power State, Management IP, Host name, Service Tag, OS, DNS DRAC Name, Processors, and Memory.
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**
   - **Network Interfaces**
   - **Firmware Revisions**
   - **CPUs**

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. In the left pane, click **Resources**.
   The **Resources** page is displayed.
2. In the **All Resources** tab, click VMware vCenter from the resource list to view the details.
   The **Details** pane in the right displays the basic information about the VMware vCenter, such as Power State, Management IP, Datacenters, Clusters, Hosts, and Virtual Machines
3. Additionally, in the **Details** pane, under **vCenter Details**, click the arrows to expand **vCenter** → **Datacenter** → **Cluster** to view the lists of nodes and application.

Viewing SCVMM details

1. In the left pane, 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:
   - Power State
   - Host Groups
   - Clusters
   - Hosts
   - Virtual Machines
3. Additionally, 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 application.

Viewing storage group details

1. In the left pane, 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.

   The **Details** pane in the right displays 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 8.0 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.

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. In the left pane, 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** in the right, 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** in the right, 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
Editing server pool
Editing server pool
Application logs
Users
Repositories
About roles
Scheduled jobs
Virtual appliance management

Creating server pool

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

Editing server pool

1. In the **Server Pools** tab, click **Edit**.
   The **Create Server Pool** wizard is displayed.
2. To change the name and description of the server pool, in the left pane, click **Server Pool Information**. Click **Save**.

3. To add or remove servers from the server pool, in the left pane, click **Add Servers**. Click **Save**.
4. To add or remove the access rights to the server pool, in the left pane, click **Assign Users**. Click **Save**.

Related Links

Creating server pool
Editing server pool
Application logs
Users
Repositories
About roles
Scheduled jobs
Virtual appliance management

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

- Configure automatically scheduled and manual backup and restore jobs.
- Create the credentials that ASM will 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

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. Additionally, it is recommended to take a snapshot of ASM virtual appliance every time you perform a restore (for more information, refer to 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 required
- Backup Directory User Name

Additionally, 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. In the left pane, 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 will be 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. In the left pane, 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. In the left pane, 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 will be 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. Additionally, it is recommended to take a snapshot of ASM virtual appliance every time you perform a restore (for more information, see VMware documentation).

1. In the left pane, 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 into 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
Deleting credentials

Creating credentials

To create new credentials:

1. In the left pane, 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**
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 and SCVMM, 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. In the left pane, 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. In the left pane, 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.

Related Links

Creating credentials
Editing credentials

Getting Started

This page provides a recommended guided workflow for getting started with ASM. A check mark indicates that you have completed the step. For more information, see Getting started with ASM 8.0

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 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. In case of 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.

Related Links

Exporting all log entries
Purging log entries

Exporting all log entries

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

1. In the left pane, 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. In the left pane, 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**, and **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 select either a date or at least one severity level.

Networks

ASM manages LAN (private, public, and hypervisor management), hypervisor migration, hypervisor cluster private, PXE, File Share, and SAN (iSCSI/FCoE) networks.

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

Additionally, make sure that the following network prerequisites 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 PXE 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
- VLAN ID
- Network Type

From this page, you can:

- Define a network
- Edit an existing network
- Delete a network

Additionally, 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.

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. In the left pane, 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]
   - SAN [FCoE]
   - Hypervisor Management
   - Hypervisor Migration
   - Hypervisor Cluster Private
   - PXE
   - Fileshare
   - FIP Snooping
   - 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.
   - For an FCoE network type, a virtual FIP 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: Currently, stating IP addressing is not supported for SAN [FCoE] network types.

   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
Deleting a network

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.
- **SAN (FCoE)**— Used to identify storage-related traffic on a Fibre Channel Over Ethernet (FCoE) network.
- **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 another node in the same cluster.
- **Hypervisor Cluster Private**— Used for private cluster heartbeat network communication.
- **PXE** — Used to manage Preboot Execution Environment (PXE) network for OS imaging on servers.
- **Fileshare** — Used to manage the NFS traffic in the NetApp Storage file system.
- **Fileshare** — Used to manage the NFS traffic in the NetApp Storage file system.

- **Hardware Management**— Used for out-of-band management of hardware infrastructure.
- **FIP Snooping**— Fibre Channel over Ethernet (FCoE) Initialization Protocol (FIP) snooping provides security mechanism that prevents unauthorized access and data transmission to a Fibre Channel (FC) network.

  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 will affect the services that will be deployed using this template.

To delete a network:

1. In the left pane, 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

Network types
Network types
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 tab** – Enables you to create Firmware Repositories.

Related Links

Understanding Firmware tab
OS Image repositories

OS Image 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.

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

Adding OS Image repositories

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.

Understanding Firmware tab

The **Firmware** 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.
- **Set as Default** — The check mark next to the repository indicates that it is a default repository.
- **Deployed** — The possible values are:
  - **Yes** — Indicates that the catalog is part of a service.
  - **No** — Indicates that the catalog is not part of any service.

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 the repository from the list, and click **Remove** to remove a repository.

  NOTE: If you remove a repository, the repository is deleted from the appliance not from the file share.
- Select a repository from the list, and click **Set as Default Repository** to set a repository as a default repository
- Click **Configure Settings** to compare the default repository with the latest package available at Dell.com
- In the right pane, click **View Bundles** to view the firmware bundles available in the repository.

Related Links

Adding firmware repositories

Viewing firmware bundle 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, FTTP, 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**.

Viewing firmware bundle details

Displays the firmware update packages available in the bundle:

- **Name** — Displays the name of the firmware update package.
- **Version** — Displays the version of the firmware update package.

- **Date** — Displays the date when the firmware update package was downloaded.
- **Size** — Displays the size of the firmware update package.

Scheduled jobs

NOTE: User with Administrator role can only view and cancel the jobs. Currently, Standard users are not allowed to cancel the jobs that they have scheduled.

In ASM, you can view the details of the following jobs and cancel the jobs:

- Discovery
- Firmware Update
- Inventory
- Service Deployment
- Chassis Configuration

The **Scheduled 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 **Scheduled Jobs** page.

From this page, you can cancel the job that is currently running.

To cancel the job:

1. On the **Schedule Jobs** page, in the **State** column, select the check box next to job that you want to cancel.
2. Click **Cancel** to cancel the jobs.

Users

The **Users** page allows you to manage the users within ASM. You can create a new 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.

Additionally, you can click on 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 a new ASM user. Enter the following information to create a new user.

1. On the left pane, 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 will enter 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, and one special character.
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 users

Deleting a user

The Delete option allows you to remove an existing ASM user. Perform the following tasks to delete a user:

1. In the left pane, 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. In the left pane, click **Settings**, and then click **Users**.
2. On the **Users** page, select a single user account to edit.
3. Click **Edit**.
4. Modify the user account information.
5. Click **Save**.

Related Links

Users
Creating a user
Deleting a user
Enabling or disabling users
Importing 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 below to enable or disable the user account state:

1. In the left pane, 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 into 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. In the left pane, 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 refer to 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
Summary
Importing users
Connection settings matrix

Attribute settings matrix

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**.

Related Links

Connection settings
Summary
Connection settings matrix
Attribute settings matrix
Connection settings
Summary
Connection settings matrix
Attribute settings matrix

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.

Field Name	Description
	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. In the left menu, 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. In the left pane, 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 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 software:

NOTE: Prior to importing Active Directory users, you must create at least one directory service through 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. 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.

1. In the left pane, click **Settings** and then click **Users**.
2. In the **Users** tab, click **Import Active Directory Users**.
3. Select a specific directory service from the **Select Directory Service** drop-down list, to import the users from the selected directory service.
4. Select one or multiple users to be imported from the **Directory Users List** (displays the list of users existing in the selected directory service), and click the forward arrow button, to add the selected users to the **Selected Users List** (displays the **Name**, **First Name**, **Last Name** and **Role** of the selected users to be imported).
5. Select one or multiple users in the **Selected Users List** and click **Apply** to import the users.

   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 level to each imported user.

   NOTE: In the **Selected Users List**, each User Name is prefixed with a check box. Selecting this check-box will allow you to *Select Role* to change the role of the selected user(s), from the **Change Roles** drop-down list that appears on the top right of the **Selected Users List** box. By selecting this check box, you can also revert the users back to the **Selected Directory Users List** box. However, the selection of these pre-fixed check boxes in the **Selected Users List** does not allow you to **Apply** only the selected users. On clicking **Apply**, all users get applied, irrespective of check-box selection.

   NOTE: An active directory user is authenticated against the specific active directory that a user belongs to.

About roles

Every ASM user account can be assigned to any one of the following roles:

- Administrator — Users with Administrator role has the privilege to view all the pages and to perform all operations in ASM and grant permission to Standard user to perform certain operations.
- Standard — Users with Standard role can view certain pages and perform certain operations based on the permission granted by Administrator. Additionally, Standard users can grant permission to other user to view and perform certain operation that they own.
- Read Only — Users with Read Only role can view all ASM operations but not allowed to perform any operation. 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:

Feature	Permission	Roles			Notes
		Administrator	Standard	Read-only	
Dashboard	View	Y	Y*	Y	*Standard users are allowed only to view the services, templates, resources and pools utilized, and recent activity that they have created or for which they have permission.
	View Service Details	Y	Y*	Y	*Standard users are allowed only to view the details of the services that they created or for which they have permissions.
	Access Recent Templates	Y	Y*	N	*Standard users are allowed only to view the recent templates that they have created.
Services	View	Y	Y*	Y	*Standard users are allowed only to view the services that they have created or for which they have permissions.
	Deploy Service	Y	Y*	N	*Standard users are allowed only to deploy services that they have created or have permissions.
	Export Service Details	Y	Y*	N	*Standard users are allowed only to export only the details of the services that they have created or have permissions.

Service Details	View	Y	Y*	Y	*Standard users are allowed only to view only the details of the services that they have created or have permissions.
	Open Resource Console	Y	Y*	N	*Standard users are allowed only to view only the details of the resources that are part of the pool for with they have permissions.
	Edit Service Informati on	Y	Y*	N	*Standard users are allowed only to edit only the service that they have created.
	Delete	Y	Y*	N	*Standard user are allowed only to delete o the service that they have deployed.
	Cancel	Y	Y*	N	*Standard user are allowed only to cancel the service that they have deployed.
	Retry a failed service	Y	Y*	N	*Standard users are allowed only to redeploy a failed service that they have deployed.
	View Service Details	Y	Y*	Y	*Standard users are allowed only to view the details of the resources that are part of the service that they have created or have permissions.
	Add compone nt to the service	Y	Y*	N	*Standard users are allowed only to add components to a service that they have permission.
	Migrate servers	Y	Y*	N	*Standard users are allowed only to migrate the servers that are part of the server pool for with they have permission.
	View firmware complian ce report	Y	N	N	
Templates	View	Y	Y*	Y	*Standard users are allowed only to view the templates for which administrator has granted the permissions.

	Create new template	Y	N	N	
	Edit template	Y	N	N	
	Delete template	Y	N	N	
	View template details	Y	Y*	Y	*Standard user are allowed only to view the details of the template for which they have permission.
	Clone template	Y	N	N	
Template Edit	View	Y	N	N	
	Edit name/ category/ description	Y	N	N	
	Publish template	Y	N	N	
	Delete template	Y	N	N	
	View All Settings	Y	N	N	
	Import template	Y	N	N	
Resources	View	Y	*Y	Y	*Standard users are allowed only to view the resources that are part of a service pool for which they have permissions. However, the user can view the shared resources that are not in a pool.
	Discover resources	Y	N	N	
	Remove resources	Y	N	N	

	Manage or unmanage resources	Y	N	N	
	Run inventory	Y	*Y	N	*Standard users are allowed only to run the inventory on the resources that are part of the service pool for which they have permission.
	View resource details	Y	*Y	Y	*Standard users are allowed only to view only the details of the resources that are part of the service pool for which they have permission.
	Launch resource element manager	Y	*Y	N	*Standard users are allowed only to launch the element manager of the resources that are part of the service pool for which they have permission.
Server Pools	View	Y	*Y	Y	*Standard users are allowed only to view the details of the server pools for which they have permissions.
	Create	Y	N	N	
	Edit	Y	N	N	
	Delete	Y	N	N	
Settings	View	Y	N	Y	
Application Logs	View	Y	N	Y	
	Export All	Y	N	N	
	Purge	Y	N	N	
Backup and Restore	View	Y	N	N	
	Backup Now	Y	N	N	
	Restore Backup	Y	N	N	

	Edit Backup Settings	Y	N	N	
Credential Management	View	Y	N	Y	
	Create	Y	N	N	
	Edit	Y	N	N	
	Delete	Y	N	N	
Getting Started	View	Y	N	Y	
	• Initial Setup • Define Networks • Discover Resources • Configure Resources • View Templates	Y	N	N	
Networks	View	Y	N	Y	
	Define	Y	N	N	
	Edit	Y	N	N	
	Delete	Y	N	N	
Users	View	Y	N	Y	
	Create	Y	N	N	
	Edit	Y	N	N	
	Disable/ Enable	Y	N	N	
	Delete	Y	N	N	

	Import	Y	N	N	
Directory Services	View	Y	N	Y	
	Create	Y	N	N	
	Edit	Y	N	N	
	Delete	Y	N	N	
Virtual Appliance Management	View	Y	N	Y	
	Generate Troubleshooting Bundle	Y	N	N	
	Edit Time Zone and NTP Settings	Y	N	N	
	Edit Proxy Settings	Y	N	N	
	SSL Certificates	Y	N	N	
	Generate Certificate Request	Y	N	N	
	Upload Certificate	Y	N	N	
	Edit License	Y	N	N	
Virtual Identity Pools	View	Y	N	Y	
	Create	Y	N	N	
	Export	Y	N	N	

	Delete	Y	N	N	

Related Links

Creating a user
Editing a user
Deleting a user
Enabling or disabling users
Importing users

Virtual appliance management

Virtual Appliance Management allows you to:

- Generate a troubleshooting bundle
- Edit NTP settings
- 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

Generating a troubleshooting bundle
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

Generating a troubleshooting bundle

A troubleshooting bundle is a compressed file that contains appliance logging information for ASM virtual appliance. If required, you must download the bundle and send it to Dell support for issue debug.

1. In the left pane, 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 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. In the left pane, 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. In the left pane, click **Settings**, and then click **Virtual Appliance Management**.
2. On the 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. In the left pane, 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. In the left pane, 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 will replace the existing license.

1. In the left pane, click **Settings**, and then click **Virtual Appliance Management**.
2. On the **Virtual Appliance Management** page, under the **License Management** section, click **Edit**.
3. Click **Browse**, select a valid license file, and then click **Open**.
4. To activate the license, click **Save**.

   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
   - Activation Date

   (If multiple standard licenses are uploaded, details of all the licenses are displayed).

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. In the left pane, 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.

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 will be 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
Deleting virtual identity pools
Exporting 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. In the left pane, 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 less 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 **Summary** page, click **Finish**.

Related Links

Adding virtual MAC identities

1. On the **Virtual MAC** page of the Create Virtual Identity Pool wizard, in the **Number of Virtual MAC Identities** box, 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 beginning 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 required.

Adding virtual IQN identities

At a time, you can add as less as one and as many as 1,024 virtual IQN identities at one time. The maximum number of virtual IQN 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** box 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 beginning 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 required.

Adding virtual WWPN identities

At a time, you can add as few as one and as many as 1,024 virtual WWPN identities. 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** box, 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 beginning 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 required.

Adding virtual WWNN identities

At a time, you can add as few as one and as many as 1,024 virtual WWNN identities. 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 beginning 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. In the left pane, 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.

Related Links

Creating virtual identity pools
Exporting virtual identity pools

Exporting virtual identity pools

You can export the .txt file that contains the virtual identity pools information.

1. In the left pane, 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.

Related Links

Creating virtual identity pools
Deleting virtual identity pools

9

Troubleshooting

This chapter includes details for resolving common issues encountered in ASM 8.0.

For additional support information, go to http://support.dell.com/support/topics/topic.aspx/global/shared/support/prosupport/en/prosupport-software-contacts?c=us&l=en&s=biz.

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 will be 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 8.0 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 general pvid 3000

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.