Active System Manager
Version 7.5 User's Guide

Notes, Cautions, and Warnings

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

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 - 02

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 Active System Manager 7.5 features an enhanced 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.

2

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 Active System Manager (ASM), version 7.5.

On the **Manuals** page, in the **Tell us about your Dell system** section, under **No**, select **Choose from a list of all Dell products**, and then click **Continue**. On the **Select your product type** page, click **Software & Security → Enterprise System Management → Active System Manager → Dell Active System Manager 7.5**.

- *Dell Active System Manager version 7.5 Quick Installation Guide*
- *Dell Active System Manager version 7.5 Online Help*

  NOTE: You can access the online help after you install ASM.
- *Dell Active System Manager version 7.5 Release Notes*

3

Licensing

Active System Manager (ASM) licensing is based on the total number of managed resources, except for VMware vCenter. In ASM 7.5 release, standard is the only valid license type supported.

The standard license is a full-access license type.

To download a license:

1. You will receive an email from customer service with instructions to access the license file from digital locker that includes your login ID and password.
2. To view the instructions, log in to "My Locker" with your login (email address) and password.
3. To download a license to your local share, click **download**.

If you are using ASM for the first time, you must upload the license file through the **Initial Setup** wizard. You can then upload and activate subsequent licenses on the **Virtual Appliance Management** page under **Settings**. After uploading an initial license, subsequent uploads replaces the existing license.

4

Getting Started with ASM 7.5

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

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, proxy server, and networks settings. To proceed to Step 2, you must complete the initial setup configuration.

  After initial setup is complete, to edit the NTP, proxy server, and license information, click **Settings** → **Virtual Appliance Management** in the left pane. To define, edit, or delete your existing networks, in the left pane, click **Settings** → **Networks**.
- **Step 2: Discover Resources** — Click **Discover Resources** to discover one or more resources (chassis, blade server, switch, storage, and VMware vCenter instances) that you want ASM to manage on your network.
- **Step 3: Publish Template** — Click **View and 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.

When the initial setup and discovery step is 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, in the left pane, click **Settings** → **Getting Started**.

Related Links

Discovery Overview
Initial Setup
Discovering Resources
Templates

5

Initial Setup

The Initial Setup wizard enables you to configure the basic settings required to start using Active System Manager (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 addresses of at least two Network Time Protocol (NTP) servers.
- The IP address, 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. On the **Networks** page, define existing networks and click **Save and Continue**.
6. On the **Summary** page, verify the time zone, proxy server, and network settings.
7. Click **Finish** to complete the initial setup.

After the initial setup is complete, if you want to edit the NTP, proxy server, and license information, in the left pane, click **Settings → Virtual Appliance Management**. If you want to define, edit, or delete your existing network, in the left pane, click **Settings → Networks**.

Related Links

Uploading License
Configuring Time Zone and NTP Settings
Configure Proxy Settings
Networks
Configure Proxy 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, in the left pane, click **Settings** → **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, select a valid license file, and then click **Open**.
   The following information is displayed based on the license selected:
   - **Type** — Displays the license type. Standard is the only license type supported in ASM 7.5 release.
   - **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 set the time zone in which Active System Manager virtual appliance operates, and configure Network Time Protocol (NTP) servers used for time synchronization.

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, in the left pane, click **Settings** → **Virtual Appliance Management.**

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 Active System Manager (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** → **Virtual Appliance Management**.

Related Links

Editing Proxy Settings

Networks

You must at least define one network on the **Networks** page of the **Initial Setup** wizard. You can edit or delete existing networks from ASM once it is defined.

To define, edit, or delete the network after the initial setup is complete, in the left pane, click **Settings** → **Networks**.

Related Links

Defining or Editing Existing Network
Deleting a Network

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.

6

Dashboard

The **Dashboard** displays a graphical representation of the state and total number of services deployed in ASM. These services are categorized into 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 get deployed successfully.
- **In Progress Services** (BLUE band on the graphic): Indicates the services that are currently in the process of getting deployed.

To display a list of services in a particular state, click the related color band on the graphic, that is red, blue or green. This list is then displayed in the middle of the page and provides basic service details including:

- State icon:

  Error 

  Deployed 

  In Progress 

- Service name that can be clicked to view full service details.
- Name of the user who deployed the service.
- Date and time when the service was deployed.
- The number of resources per category used by that particular service.
- Errors, if any.

The **Dashboard** also displays the following:

- Total number of services running on ASM.
- State icons displaying the number of services within each service state.
- **Licensing information** (displayed when the number of resources being managed by ASM exceeds the valid license count).
- **Deploy Service from Recent Templates** option displays a list of most recent templates that have been published and are available for deployment.
- **Recent Activity** option that lists user and system initiated activities.
- Links to learn more about service deployments and templates.

On this page you can:

- Deploy a new service from published templates (For more information, see **Deploy Service**).
- Click the service name to view **Service Details** (For more information, see **Service Details**).

Related Links

Service Details
Deploy Service
Service States

Deploy Service

The **Deploy Service** dialog box enables you to deploy a service instance using a template.

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 launch the **Deploy Service** dialog box, perform one of the following actions:

- On the **Dashboard** page, click **Deploy Service**.
- On the **Templates** page, select a template, and click **Deploy Service**.

To deploy a service:

1. In the **Deploy Service** dialog box, enter the following information in the **Basic Details** tab:
   a. Enter the Service Name (required) and Service Description (optional) that identifies the service.
   b. Select the template to deploy a service from the Select Template drop-down list.
      The fields that are specifically required for deployment are displayed and must be completed for deployment.
2. Click the **Advanced Details** tab.
   The **Advance Details** tab displays the settings defined for the components in the template. You can modify the settings based on the requirement.
3. Click **Deploy Now**.

Service States

State	Icon
Error Services	
In Progress Services	
Deployed Services	

Related Links

Dashboard

Service Details

The **Service Details** page displays the following details:

- Basic Service Details: Indicates the basic details that are specific to a particular service state. These details are displayed in the middle of the **Dashboard** home page. The basic service details include:
  - State icon:

    Error 

    In Progress 

    Deployed 
  - Service name that can be clicked to view full service details.
  - Name of the user who deployed the service.
  - Date and time when the service was deployed.
- Full Service Details: Indicates additional details about a service. To view the details about a service, click a service name. A service details page is opened. The **Service Details** page displays the following:
  - State icon.
  - Name of the service.
  - Topology of components in the selected template from which the service was deployed.

    Additionally, in the topology view, click a component to view the deployment log information of the component. The red component icon indicates an error occurred while deploying the service on the particular component.
  - Basic service information, such as Description, State, Deployed By and Deployed On.
  - Details of all resources deployed using this service, in a tabular form.
  - Recent activity specific to the selected service.

NOTE: The **Delete Service** operation on this page allows you to delete a service. This action deletes the instance of the service and returns the IP/IQNs assigned to the servers that were a part of the service. On performing this action, the Dell servers that were part of the deleted service, are rebooted and are set to PXE boot ready for the next deployment. In case of non-Dell servers, you need to Power Off the server manually, for the non-Dell server to be a part of future deployments. Similarly, you need to manually Power On the servers and set the "next boot" to PXE, in case of non-Dell servers.

Related Links

Deploy Service

7

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.

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

Managing Templates
Cloning a Template
Deleting a Template
Creating a Template
Editing a Template
Building and Publishing a Template
Importing a Template

Managing Templates

The **Templates** page displays the following information about the templates:

- Representational icons of components that may be within any template. Those icons in blue are depicting which components are included in each template.
- Summary details on a selected template.

You can click on a specific template to see the following details of the selected template:

- **Created on:** This field describes the date and time of template creation.
- **Created by:** This field mentions the name of the user who created the template.
- **Updated on:** This field describes the date and time when the template was last updated.
- **Update by:** This field mentions the name of the person who last updated the template
- **Last Deployed on:** This field mentions the date and time when the selected template was last deployed.

On this page, you can:

- Create a Template
- Edit a Template
- Delete a Template
- Deploy a Template
- View Template Details
- Clone a Template

NOTE: For the templates that appear in a Draft state on the **Templates** page, the **Deploy Service** option is deactivated. To activate the **Deploy Service** option, edit the template in Draft state and publish it.

Related Links

Creating a Template
Editing a Template
Deleting a Template
Cloning a Template
Importing a Template
Deploy Service

Creating a 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. Click **Templates** → **Create Template**.
2. 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 get cloned into the new template.

3. Enter a **Template Name**.
4. Enter **Template Description**. (Optional).
5. Click **Save**.

Related Links

Building a Template Overview
Building and Publishing a Template

Building a 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:

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

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
- Edit Template name
- Delete a Template
- Import a Template
- Deploy a Service

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

Related Links

Building and Publishing a Template

Building and Publishing a Template

To start building a customized template, perform the following steps:

1. Click **Templates** → **Create Template**.
2. Select either **New** or **Clone Existing** radio button.
3. Enter a **Template Name**.
4. Enter a **Template Description**. (Optional).
5. Click **Save**.

   On the **Build Template** page, a newly created or cloned template appears in a Draft state.
6. To add components to your template, click a specific component icon in the left. From the **Select a Component** drop-down list, select the component that you want to add. Specific settings and properties appear automatically that are required and can be edited. After completion, click **Add**.
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.

   For more information about a particular type of component, see **Component Types** section.

   On the **Build Template** page, the **Deploy Service** option is not visible until you click the **Publish Template** option. On publishing, the **Edit** and **Deploy Service** options are visible.

Related Links

Building a Template Overview
Deploy Service

Importing a 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. **Create Template** or **Edit** an existing template.
3. On the Template Builder page, click **Import Template**.
4. On the right, select a specific template from the **Select a template** drop-down list, and click **Import**.

Editing a 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

Deleting a 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.

Cloning a 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

The **Deploy Service** dialog box enables you to deploy a service instance using a template.

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 launch the **Deploy Service** dialog box, perform one of the following actions:

- On the **Dashboard** page, click **Deploy Service**.
- On the **Templates** page, select a template, and click **Deploy Service**.

To deploy a service:

1. In the **Deploy Service** dialog box, enter the following information in the **Basic Details** tab:
   a. Enter the Service Name (required) and Service Description (optional) that identifies the service.
   b. Select the template to deploy a service from the Select Template drop-down list.

      The fields that are specifically required for deployment are displayed and must be completed for deployment.
2. Click the **Advanced Details** tab.

   The **Advance Details** tab displays the settings defined for the components in the template. You can modify the settings based on the requirement.
3. Click **Deploy Now**.

Components Types

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

The following component types are defined in ASM:

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

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

Application
Server
Cluster
Storage
Virtual Machine
Component Combinations

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

After selecting **Storage** on the template builder page, you can perform the following actions:

- Perform settings on *Compellent* and *EqualLogic CHAP* storage resource properties that display on the right of the page (for more information, see **Storage Settings**).

  NOTE: The **Select a Component** drop-down list allows you to select from *Compellent* and *EqualLogic CHAP* storage components, as defined in ASM. Based on your resource selection, the page displays specific resource properties for you to perform settings.
- Select **Related Components** to be mapped with the selected storage resource type (for more information about valid component combinations that can be mapped together in a template, see **Component Combinations**).
- To add a Storage Component, click **Add**.

NOTE: Currently, you can add only one instance of each storage component type while building a template.

Storage Settings

Field Name	Description
EqualLogic Chap Storage Settings	
Storage Volume	Defines 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	Refers to the 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*.
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.
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 autogenerated.
Compellent Storage Settings	
Storage Volume	Refers to the name of the volume that is to be created or destroyed.

Field Name	Description
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 for this parameter 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	Refers to the optional user notes associated with the server.
Server Object Name	Refers to the server name that is to be created or destroyed.
Operating System Name	Refers to the name of the operating system hosted on the server.
Server Object Folder	Refers to the folder for the server.
Server WWN Values	Refers to a globally unique world wide name 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 **porttype** 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*.

Server

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

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

- Perform settings on the selected server instance properties that display on the right of the page (for more information, see **Server Settings**).

  NOTE: A Server name must be unique for a given deployment.

  NOTE: The **Select a Component** drop-down list allows you to select a server instance and perform settings on the selected server instance properties that populate on selecting a server from **Select a Component** drop-down list.
- Select **Related Components** to be mapped with the selected server instance (refer to the **Component Combinations** section in the **Related Links** below, to see the valid component combinations that can be mapped together in a template).
- To add a Server Component, click **Add**.

Server Settings

Target Boot Device	Description
Hardware Settings	
Target Boot Device	Refers to the target boot device (for example: Local Hard Drive or SD card).
Server Pool	Refers to the server pool whose resource is being used. The *Global* value allows you to select any server pool from **Resources** in ASM.
OS Settings	
Administrator password	Refers to the admin password specified while configuring a server component.
Confirm administrator password	Refers to reconfirming the admin password specified while configuring a server component.
OS Image	Refers to the OS images that are available for deployment. These OS images are installed by the customer or support personnel. They are the actual ISOs.
OS Image Type	Refers to the operating system types (for example: Red Hat, Linux, Windows) 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.
Network Settings	
Identity Pool	Refers to the Identity Pool that is used to connect to the storage devices. Selecting a *Global* value here allows you to choose the identities or MAC addresses, IQNs, WWNNs and WWPNs.
Host Name	Refers to the Host Name set during deployment.

Target Boot Device	Description
Hypervisor Management Network	(Optional networks) Refers to all networks of the type “Hypervisor Management”.
Hypervisor vMotion Network	(Optional networks) Refers to all Hypervisors available for vMotion.
Storage Network	(Optional networks) Refers to all SAN iSCSI and FCoE networks.
PXE Network	Refers to configuring the PXE based OS imaging on servers. The specified VLAN is configured as un-tagged VLAN on the ToR/IOA switches.
Workload Templates	Refers to all the private and public networks in the network stage. You can choose multiple networks. However, it is mandatory to select at least one network.

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).

Cluster

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

NOTE: Currently in ASM, cluster creation for hyperV is not supported.

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

- Perform settings on the selected cluster instance properties that display on the right of the page (for more information, see **Cluster Settings**).

  NOTE: The **Select a Component** drop-down list allows you to select a cluster instance and perform settings on the selected cluster instance properties that populate on selecting a specific cluster from **Select a Component** drop-down list.
- Select **Related Components** to be mapped with the selected cluster instance (for more information about the valid component combinations that can be mapped together in a template, see**Component Combinations**).
- To add a Cluster Component, click **Add**.

Cluster Component Settings

Field Name	Description
Cluster Settings (Target vCenter)	
Data Center Name	Refers to the name of the data center to be created in vCenter. The keyword cluster is not required.
Cluster Name	Refers to the name of the cluster to be created in the Data Center.

Field Name	Description
Cluster Data Store	This property maps the cluster to the selected storage component.

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, you can perform the following actions:

- Perform settings on Virtual Machine properties that display on the right of the page (for more information, see **Virtual Machine Settings**).

  NOTE: From the **Select a Component** drop-down list, you can select a Virtual Machine instance. Based on your selection, the page populates specific resources properties for you to perform settings on Virtual Machine instance.

- Select **Related Components** to be mapped with the Virtual Machine instance (refer to the **Component Combinations** section in the **Related Links** below, to see the valid component combinations that can be mapped together in a template.)
- To add a Virtual Machine, click **Add**.

Virtual Machine Settings

Field Name	Description
Virtual Machine Settings	
Number of CPUs	Refers to the number of CPUs specified while configuring a Virtual Machine.
Memory in MB	Refers to the memory in GB specified while configuring a Virtual Machine.
Number of NICs	Refers to the number of NICs specified while configuring a Virtual Machine.
Virtual Machine OS Settings	
Administrator password	Refers to the admin password specified while configuring a Virtual Machine.
Confirm administrator password	Refers to reconfirming the admin password specified while configuring a Virtual Machine.
OS Image	Refers to the OS images that are available for deployment. These OS images are installed by the customer or support personnel. They are the actual ISOs.
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.

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** on the template builder page, you can perform the following actions:

- Perform settings on the selected application properties that display on the right of the page (the properties of each application vary based on the application type).

  NOTE:

  From the **Select a Component** drop-down list, you can select any application from the list of defined applications in ASM. Based on your selection, the page displays the application properties for you to perform settings. After selecting a component, the component properties page is displayed.
- Select **Related Components** to be mapped with the selected application (for more information about the valid component combinations that can be mapped together in a template, see **Component Combinations** section in the **Related Links**.)
- To add a Server Component, click **Add**.

Component Combinations

	Valid Component Mappings								
Application					X				X
Virtual Machine				X	X			X	X
Cluster			X	X	X		X	X	X
Server		X	X	X	X	X			
Storage	X	X	X	X	X				

8

Resources

The Chassis, servers, switches, storage groups, and VMware Centers that you can manage using Active System Manager 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.

Related Links

Understanding All Resources Tab
Understanding Server Pools

Understanding All Resources Tab

The **All Resources** tab displays the following information in tabular form about the resources discovered and managed in Active System Manager (ASM).

- State in which the resource exists. For example, powered on, powered off, deployed, 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.

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 **View By** drop-down list, select one of the following resource types:

- **All Resources**
- **Dell Chassis**
- **Servers**
- **Switches**
- **Storage**
- **vCenter**

From this page, you can:

- Discover new resources
- Update the resource inventory
- Remove resources
- View resource details

Related Links

Discovery Overview
Discovering Resources
Viewing Resource Details
Removing Resources
Updating Resource Inventory
Resource Operational State

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 Active System Manager 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**, and then click **Discover** in the **Resources** → **All Resources** tab.

Related Links

Discovering Resources

Discovering Resources

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

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

NOTE: For 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 **Discover Resources** page, click **Add New**.
3. In the **Add IP Address Range** dialog box, perform the following steps, and click **Save**.
   a. Type the IP address range of the resources that you want to discover.
   b. Select the resource types that you want to discover within the specified IP address range.
   c. Select the credentials corresponding to the resource types.
4. To add multiple IP address ranges, repeat the steps 2 and 3, and then click **Next**.

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

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 Range and Credentials

1. On the **Discover Resources** page, click **Add New**.
2. In the **Add IP Address Range** dialog box, perform the following steps, and click **Save**.
   a. Type the **Starting IP Address** and **Ending IP Address** (optional) of the resources range that you want to discover.
   b. Under **Include Resources**, select the resources types.

      Active System Manager discovers only the selected resource types within the specified IP address range.
   c. Select the Dell default credentials or existing credentials from the corresponding resource credentials drop-down list. ASM uses the specified credentials to access the resources.
   d. To use new credentials to access the resources, click **Add New** next to the corresponding credentials types.

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

Related Links

Add IP Address Range Dialog Box Options

Add IP Address Range Dialog Box Options

Field Name	Description
Starting IP Address	Type the Starting IP Address of the resource range. NOTE: To discover single resource, enter only the starting IP address.
Ending IP Address	(Optional) Type the ending IP Address of the resource range.
Include Resources	Select the following check boxes next to the resource type. ASM discovers only the corresponding resource types within the specified IP address range. • **Dell Chassis (Chassis, Blade Servers, I/O Modules)** • **Servers** • **Storage** • **Switches** • **vCenter**

Field Name	Description
Chassis Credentials	Select the credentials from the following drop-down lists to access one or more chassis, associated blade servers, and I/O modules. • **Chassis Credentials** • **Blade Credentials** • **I/O Module Credentials** If you want to create new credentials to access the chassis, click **Add New**. NOTE: The options to select or create new credentials are displayed based on the resource types selected for discovery.
Server Credentials	Select the credentials from the drop-down list to access one or more Servers. If you want to create new credentials to access the servers, click **Add New**.
Storage Credentials	Select the credentials from the drop-down list to access one or more Storage resources. If you want to create new credentials to access the storage resources, click **Add New**.
Switch Credentials	Select the credentials to access one or more switches. If you want to create new credentials to access the switches, click **Add New**.
vCenter Credentials	Select the credentials to access one or more VMware vCenter servers. If you want to create new credentials to access the VMware vCenter resources, click **Add New**.

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.

Removing Resources

To remove any particular resource from Active System Manager (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 a 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

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.

Viewing Resource Details

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 7.5 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 Switch Details
Viewing VMware vCenter Details

Viewing Chassis Details

1. In the **Resources** → **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.
2. 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 **Resources** → **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, Location, OS, DNS DRAC Name, Processors, and Memory.
2. 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 **Resources** → **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
2. 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 Storage Group Details

1. In the **Resources** → **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.
2. 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 7.5 release, the detailed information can be viewed only for Dell Resources.

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

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

Viewing Switch Details

1. In the **Resources** → **All Resources** tab, click a switch from the list of resources to view it details.
   The **Details** pane in the right displays the basic information about the switch, such as Power State, Management IP, Host name, Service Tag, and Location.
2. In the **Details** pane, click **View Details**.
   The **Switch** details page displays more information about the switch in the **Summary** tab.

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

From the **Switch Details** page, you can view recent activity performed on the switch.

Related Links

Viewing Chassis Details
Viewing Blade or Rack Server Details
Viewing Storage Group Details
Viewing VMware vCenter Details

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 Active System Manager:

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 Active System Manager (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**.

Resource Operational State

After initiating the resource discovery, Active System Manager (ASM) assigns one or more of the following states to the resources. These operational states display in the **State** columns of the **Resources** → **All Resources** tab.

State	Description
Available	Ready to be used.
Deploying	Indicates deployment is in progress.
Pending	Indicates the following tasks are in progress: • Discovering resources is in progress. • Determining resource details • Validating support for resource details such as firmware version • Applying template to the resource • Updating firmware • Removing resource from ASM.
Powering On	Indicates the resource is powered on.
Powering Off	Indicates the resource is powered off.
Errors	Indicates an error encountered while executing the last job on the resource.
Unknown	Indicates Active System Manager does not support resources of this type, configuration, make, and/or model.

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:

- 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

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

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.

9

Settings

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

- Access application logs.
- 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.
- Define existing networks.
- Manage Active System Manager (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

Application Logs

Active System Manager 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 Active System Manager 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** → **Application Logs**.
2. 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** → **Application Logs**.
2. 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.

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 Active System Manager 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 Active System Manager 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

Active System Manager 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** → **Backup and Restore**.
2. In the **Settings and Details** section, click **Edit**.
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** → **Backup and Restore**.
2. In the **Automatically Scheduled Backups** section, click **Edit**.
3. To schedule automatic 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** → **Backup and Restore**.
2. 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 Active System Manager virtual appliance returns user-created data to a earlier configuration that is saved in a backup file.

CAUTION: Restoring an earlier configuration restarts Active System Manager 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 Active System Manager virtual appliance every time you perform a restore (for more information, see VMware documentation).

1. In the left pane, click **Settings** → **Backup and Restore**.
2. Click **Restore Now**.
3. Type a path name in the **Backup Directory Path** 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

Active System Manager (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** → **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** → **Credentials Management**.
2. On the **Credential 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**
   - **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, 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** → **Credentials Management**.
2. In 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** → **Credentials Management**.
2. In 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

Networks

Active System Manager (ASM) manages LAN (private /public /hypervisor management) 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** → **Networks** page displays information about networks defined in Active System Manager (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** → **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 [iSCSI]
   - SAN [FCoE]
   - Hypervisor 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. For a SAN (iSCSI) and Hypervisor Management network, select **Configure static IP address ranges** check box, and then do the following:

   NOTE: After a network is created, you cannot select or clear the **Configure static IP address pools** 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.

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** → **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

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 **Settings** → **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:

- 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. Click **Settings** → **Users** in the left pane.
2. Click **Create**.
3. Enter a unique **User Name** to identify the user account.
4. Enter a **Password** that a user will enter to access Active System Manager. 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. Select a **Role**.
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. Click **Settings** → **Users** in the left pane.
2. Select one or more user accounts to delete.
3. Click **Delete**.
4. 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. Click **Settings** → **Users** in the left pane.
2. 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. Click **Settings** → **Users** in the left pane.
2. 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 **Settings** → **Users** → **Directory Services** screen displays the following information about the Active System Manager 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

Connection Settings

1. Click → **Users** → **Directory Services**.
2. 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 (Bind DN)**, **Password**, **Host**, **Port** and **Protocol** (*Plain* or *SSL*) of the Active Directory that is to be added to ASM.
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 AD configuration name as added in ASM.
User Name (Bind DN)	Refers to the full distinguished name (DN), including the common name (CN), of an Active Directory user account, that has the privileges to search for users. This user account must at least have the user privileges.
Password	Refers to the AD server password.
Host	Refers to the AD server hostname or IP address.
Port	Refers to the AD server port.
Protocol	Refers to the protocol type as *Plain* or *SSL*.

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.
Filter	Refers to the filters that enable you to define search criteria.
User Name Attribute	Refers to the active directory record attribute that represents the User Name attribute. This attribute will be mapped to ASM User Name attribute.

Field Name	Description
First Name Attribute	Refers to the active directory record attribute that represents First Name. This attribute will be mapped to the ASM First Name attribute.
Last Name Attribute	Refers to the active directory record attribute that represents the Last Name of the user. This attribute will be mapped to ASM Last Name attribute.
Email Attribute	Refers to the active directory record attribute that represents the Email of the user. This attribute will be mapped to ASM Email attribute.

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. Click **Settings** → **Users** → **Directory Services**.
2. 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. Click **Settings** → **Users** → **Directory Services**.
2. 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: Before importing users from Active Directory, make sure you create a Directory Service.

1. Click **Settings** → **Users** in the left pane.
2. 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: 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

The following user roles are available in ASM:

- **Operator**: An Operator can perform the following operations in ASM:
  - Deploy a published service template on the discovered resources.
  - Click the IP Address of the resources in the **Resource** tab to link and launch the resource remote console.
  - Run Inventory.
  - Export Application Logs.
  - Create Troubleshooting bundle.
  - View recent activities

  NOTE: The Operator in ASM can view all the information that an administrator can view. However, the configuration operations for an Operator in ASM are restricted to the ones mentioned here. For the operations that an Operator cannot perform in ASM, the software restricts an Operator user from doing so by deactivating such operations.
- **Admin**: Privileged to perform all operations in ASM.
- **Read Only**: A user with a Read Only permission can view all ASM operations but cannot perform any action on any ASM operations. When a user logs in as a Read Only user, ASM does not allow the user to perform any operations by deactivating the functionality on the UI console.

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 proxy server settings
- Generate and download a Certificate Signing Request (CSR) and upload the resulting SSL certificate
- Upload an Active System Manager 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

Generating a Troubleshooting Bundle

A troubleshooting bundle is a compressed file that contains appliance logging information for Active System Manager 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** → **Virtual Appliance Management**.
2. 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 Active System Manager 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 Active System Manager.

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** → **Virtual Appliance Management**.
2. In 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 Active System Manager.

1. In the left pane, click **Settings** → **Virtual Appliance Management**.
2. In 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 Active System Manager.

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** → **Virtual Appliance Management**.
2. In 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 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** → **Virtual Appliance Management**.
2. In 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

Active System Manager 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** → **Virtual Appliance Management**.
2. In 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 Active System Manager 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** → **Virtual Appliance Management**.
2. In 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 Active System Manager (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 a 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** → **Virtual Identity Pools**.
2. On 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
Adding Virtual IQN Identities
Adding Virtual WWPN Identities
Adding Virtual WWNN Identities

Adding Virtual MAC Identities

1. On the **Virtual MAC** page of the Create Virtual Identity Pool wizard, in the **Number of Virtual MAC Identities** box, type the total number of virtual MAC identities that you want to add (any whole number between 1–1,024).
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 1–1,024).
2. In the **IQN Prefix** box, type the IQN prefix that to be added to 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 – 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 – 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** → **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 **Virtual Identity Pools**.
2. On the **Pools** page, click **Export**.
3. Open or save the file.

Related Links

Creating Virtual Identity Pools
Deleting Virtual Identity Pools

10

Troubleshooting

This chapter includes details for resolving common issues encountered in Active System Manager.

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.

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 service using the template with two EqualLogic CHAP components

Unable to deploy a service using the template with two EqualLogic CHAP components.

In ASM 7.5 release, you cannot create a template with two EqualLogic CHAP components and deploy service.

Unable to log in through Active Directory using “\”

You cannot log in through Active Directory with the domain name and username separated by back slash “\”.

To log in through Active Directory, use forward slash “/”. For example: <domain>/ <username>.

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.