# Active System Manager
# Version 7.6 User's Guide

# Notes, Cautions, and Warnings

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

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

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

# Contents

# Overview

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

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

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

**What can you do with ASM?**

ASM provides capabilities and benefits that allow organizations to:

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

**How is ASM different?**

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

- **Template-based provisioning and orchestration** — Simplify IT service delivery with a centralized approach for capturing and applying workload-specific configuration and best practices; plus step-by-step definition and execution of tasks across the workload lifecycle.
- **Infrastructure lifecycle management** — Easily manage the entire infrastructure lifecycle with:

  - Fast discovery, inventory, and initial configuration of assets.

- Full lifecycle management of physical and virtual infrastructure and workloads.
- **Deep virtualization integration** — Manage cluster-level and virtual machine (VM) lifecycle.
- **Resource pooling and dynamic allocation** — Optimize capital expenditures by creating and managing physical and virtual IT resource pools.
- **Radically simplified management** — Powerful and intuitive user interface that makes it easy to set up, deploy, and manage your IT environment and enables simplified integration with third party tools.
- **Open and extensible** — An architecture that integrates with the IT of today and tomorrow; this means being able to plug a new solution into your existing architecture, as well as giving you flexibility in the future to adopt new technical innovations.

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

# About this Document

This document version is updated for ASM, version 7.6.

# What is New in this Release

- Support for Hyper-V Compellent (Fibre Channel).
- VMs and Application support for Hyper-V or SCVMM.
- Support for ESXi NetApp Storage.
- Ability to clone a configuration of a server and apply it to another server.
- iSCSI and Fibre Channel boot support for Windows and Linux.
- iSCSI and Fibre Channel boot service migration support for Windows and Linux.
- Support for Windows 2008 R2 deployment.
- Ability to clone Hyper-V and VMware Virtual Machine from virtual machine or template.
- Template updates including new template for SQL Server Windows 2012 Support.
- Service Mobility — Capability to migrate server's BIOS, NICs, storage connectivity, and assigned identity information to another server in a designated server pool.
- Flexible Configurations — Provides multiple implementation choices for both network card and fabric configuration.
- Service Lifecycle Enhancements supports:

  - Ability to scale up storage, hosts, and virtual machines.
  - Ability to retry and deploy a failed service.

# Accessing Online Help

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

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

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

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

## Other Documents You May Need

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

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

- *Dell Active System Manager version 7.6 Release Notes*
- *Dell Active System Manager version 7.6 Quick Installation Guide*

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

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

## Licensing

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

ASM 7.6 supports following license types:

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

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

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

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

# 2

# Getting Started with ASM 7.6

When you log in to ASM for the first time, the **Getting Started** page is displayed. This page provides a recommended guided workflow for getting started with ASM. A 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, and proxy server settings. To proceed to Step 2, you must complete the initial setup configuration.

  After initial setup is complete, to edit the NTP, proxy server, and license information, click **Settings** in the left pane, and the click **Virtual Appliance Management**.
- **Step 2: Define Networks** — Click **Define Networks** to define networks that are currently configured in your environment for resources to access. To define, edit, or delete your existing networks, in the left pane, click **Settings** in the left pane, and then click **Networks**.
- **Step 3: Discover Resources** — Click **Discover Resources** to discover one or more resources (chassis, blade server, switch, storage, and hypervisor management software instances) that you want ASM to manage on your network.
- **Step 4: 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 are complete, you can still discover resources, create or edit templates, and publish templates from the left pane.

If you do not want to view the **Getting Started** page when you log in next time, clear the **Show welcome screen on next launch** check box at the bottom of the page. However, to revisit the **Getting Started** page, click **Settings** in the left pane, and then click **Getting Started**.

**Related Links**
> [Discovery Overview](#)
> [Initial Setup](#)
> [Discovering Resources](#)
> [Templates](#)
> [Defining or Editing Existing Network](#)

# 3

# Initial Setup

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

Before you begin, gather the following information:

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

To configure the basic settings:

1. On the **Welcome** page, read the instructions and click **Next**.
2. On the **Licensing** page, select a valid license and click **Save and Continue**.
3. On the **Time Zone and NTP Settings** page, configure the time zone of the virtual appliance, add the NTP server information, add then click **Save and Continue**.
4. (Optional) On the **Proxy Settings** page, select the **Use a proxy server** check box, enter the configuration details, and then click **Save and Continue**.
5. On the **Summary** page, verify the time zone, proxy server, and network settings.
6. 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, click **Settings** in the left pane, and then click **Virtual Appliance Management**.

**Related Links**
> [Uploading License](#)
> [Configuring Time Zone and NTP Settings](#)
> [Configure Proxy Settings](#)

# Uploading License

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

1. On the **Licensing** page of the Initial Setup wizard, select a valid license file, and then click **Open**. The following information is displayed based on the license selected:
   - **Type** — Displays the license type. There are two valid license types supported in ASM:
     - Standard — Full-access license type.
     - Trial — Evaluation license that expires after 90 days it supports up to 25 resources.
   - **Total Resources** — Displays the maximum number of resources allowed by the license.
   - **Expiration Date** — Displays the expiry date of the license.
2. Click **Save and Continue** to activate the license.

**Related Links**

> License Management

# Configuring Time Zone and NTP Settings

On the **Time Zone and NTP Settings** page of the **Initial Setup** wizard set the time zone in which ASM 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, click **Settings** in the left pane, and then click **Virtual Appliance Management.** . On the **Virtual Appliance Management** page, click **Edit** in the **Time Zone and NTP Settings** section.

**Related Links**

> Editing Default Time Zone and NTP Settings

# Configure Proxy Settings

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

To enable communication through a proxy server:

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

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

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

**Related Links**

    [Editing Proxy Settings](#)

# 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.

# Dashboard

The **Dashboard** displays the following information:

- Under **Service Overview** section, displays a graphical representation of the services based on their state, total number of services deployed, and state icons that represent the service state. The number next to each state icon indicates how many services are in a particular state. The services are categorized 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 are deployed successfully.
  - **In Progress Services** (BLUE band on the graphic): Indicates the services for which deployment is in progress.

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

  * State icon:

    | | | |
    |---|---|---|
    | **Error** | ❌ | Indicates service deployed is failed due to some issues. |
    | **In Progress** | 🕐 | Indicates service deployment is in progress. |
    | **Deployed** | ✅ | Indicates service deployed is completed successfully. |

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

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

  * **All Deployments**

- \* **Last 10 Deployments**
- \* **Last Week**
- \* **Last Month**
- \* **Last 6 Months**
- \* **Last Year**

- Under **Total Server Utilization**, a pie chart displays the total number of servers used and available in percentage.

  - **Servers in Use** (BLUE band on the pie chart) — Indicates the percentage of servers that are in use. To view the number of servers used, move the mouse pointer over the band.
  - **Servers Available** (GRAY band on the graphic) — Indicates the percentage of servers that are available for deployment. To view the number of servers that are available, move the mouse pointer over the band.

- Under **Utilization by Server Pool**, each bar represents a server pool and displays the number of servers used and available in that server pool.

- Under **Total Storage Capacity**, a pie chart displays the total storage capacity utilized and available in percentage.

  - **Storage Used** (BLUE band on the graphic) — Indicates total used storage disk space in percentage. To view the percentage of used storage disk space, move the mouse pointer over the band.
  - **Storage Available** (GRAY band on the graphic) — Indicates total available storage space in percentage. To view the percentage of available storage space, move the mouse pointer over the band.

- Under **Capacity by Storage Group**, each bar represents one of the following storage groups and displays the storage capacity used or available on the particular storage group.

  - **Dell EqualLogic Group**
  - **Dell Compellent Arrays**
  - **NetApp Arrays**

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

- **Licensing Information** — Displayed when the number of resources managed by ASM exceeds the valid license count.
- **Deploy Service from Recent Templates** — Enables you to view the most recent published templates and use it for deployment.
- **Recent Activity —** Lists the most recent user and system initiated activities.
- Links to learn more about service deployments and templates.

On this page, you can:

- Click the service name to view the details information about the service. (For more information, see Viewing Service Details.

**Related Links**
>  Viewing Service Details
>  Deploy Service
>  Service States

# Service States

| State | Icon | Description |
| --- | --- | --- |
| Error | | Indicates service deployment failed. |
| In Progress | | Indicates service deployment is in progress. |
| Deployed | | Indicates service is successfully completed. |

**Related Links**

[Dashboard](#)

# 5

# Services

A service is a deployment of a published template.

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

- **Error Services** — Indicates the services for which the deployment process is incomplete due to errors.
- **Deployed Services** — Indicates the services that are deployed successfully.
- **In Progress Services** — Indicates the services for which deployment is in progress.

To switch between Graphical and Tabular view, click the Graphics or Table icon  on the top-right corner of the **Services** page.

To view the services based on a particular service state, select one of the following options from the **View By** drop-down list.

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

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

In the Tabular view, the following information about the service is displayed.

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

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

- Service name and description to identify the service.
- Name of the user who deployed the service.
- Date and time when the service is deployed.
- Displays the name of the reference template used in the service.

- Lists the number of resources included in the service for deployment, based on the following component types:

  - Application
  - Virtual Machine
  - Cluster
  - Server
  - Storage

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

- Click **View Details** in the right pane to view more details about the service

- Export service details to **.csv** file.

**Related Links**

Viewing Service Details

# Viewing Service Details

The **Summary** tab displays the state of the service at component level in Topology and Tabular view.

To switch between Topology and Tabular view, click the topology or graphic icon [icon] on the top-right corner of the **Services** page.

- In the Topology view, under **Service Resources**, you can view the topology of the components, as structured in a specific/selected service template. The red component icon indicates the service is not deployed on a particular component due to some issues. The blue component icon indicates the service is successfully deployed on the components. The light blue component icon indicates the service deployment is in progress.

  To view the IP Address and Hypervisor IP Address deployed on the server, click the corresponding component icons.

- In the Tabular view, under **Service Resources**, the following information is displayed:

  - **IP Address** — Displays IP address of the resource. (Click the IP address of a Dell resource to open the Element Manager.)
  - **Hypervisor IP Address** —For servers, displays the IP address of the Hypervisor deployed on the server.
  - **Asset/Service Tag** — Displays the unique identification of a resource in the form of service tag, host name, or FQDN based on the resource types.
  - **Manufacturer** — Displays the manufacturer name. For example, Dell, Cisco, VMware, and so on.
  - **Model** — Displays the model name of the resource. For example, M620, M1000e, PowerEdge VRTX, and so on.

Additionally, in the **Storage** table, you can view the volumes and volume size configured on a particular storage. In the **Virtual Machine** table, you can view the following information about the virtual machines:

- **Hostname**
- **OS Type**
- **CPUs**
- **Disk Size**
- **Memory**

- Under **Service Information**, you can view the following information:

  - Name of the service
  - State of the service

| Service State | Icon | Description |
|---|---|---|
| In Progress | 🕐 | Indicates service deployment is in progress. |
| Error | ❌ | Indicates service deployment is failed due to some issues. |
| Deployed | ✅ | Indicates service deployment is completed successfully. |

  - Name of the user who deployed the service.
  - Date and time when the service is deployed.
  - Displays the name of the reference template used in the service.
  - Under **Recent Activities**, you can view the deployment status of the resources that are part of the deployed service, based on the component types. For more details about the deployment state. See Component Deployment States

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.

From this page, you can:

- Migrate server's settings to another server in a designated server pool.
- Redeploy a failed service.
- Add components to an existing service deployment.

The **Settings** tab displays the properties of the components that are part a service.

- For more details about the Storage properties, see Storage Settings
- For more details about the Server properties, see Server Settings

- For more details about the Cluster properties, see [Cluster Settings](#)
- For more details about the Virtual Machine properties, see [Virtual Machine Settings](#)
- For more details about the Application properties, see [Application Settings](#)

**Related Links**

    [Deploy Service](#)
    [Exporting Service Details](#)
    [Redeploying Failed Service](#)
    [Adding Components to Existing Service Deployments](#)
    [Deleting Service](#)

## Component Deployment States

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

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

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

# Deploy Service

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

To deploy a service:

1. In the left pane, click **Services**.
   The **Services** page is displayed.
2. On the **Services** page, click **Deploy New Service.**
   The **Deploy Service** dialog box is displayed.
3. In the **Deploy Service** dialog box, perform the following:

   a. From the **Select Template** drop-down list, select the template to deploy a service.

   b. Enter the **Service Name** (required) and **Service Description** (optional) that identifies the service.
4. Click **Deploy Now**.

**Related Links**

    [Adding Components to Existing Service Deployments](#)
    [Redeploying Failed Service](#)

# Deleting Service

To delete a service, perform the following steps:

1. In the left pane, click **Services**.
2. On the **Services** page, click a service, and then in the right pane, click **View Details**.
3. On the **Service Details** page, under **Actions** in the right pane, click **Delete**.

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 the servers are set to PXE boot ready for the next deployment.

After deleting the service, to avoid issues in subsequent deployments, make sure that you complete the following tasks manually:

- In case of non-Dell servers, you need to Power Off the servers, for the non-Dell server to be a part of future deployments.
- Power On the servers and set the "next boot" to PXE, in case of non-Dell servers.
- Remove any storage volumes created during the service deployment. If the volumes are no longer needed, remove the volumes from the Group Manager or Storage Center GUI.
- For EqualLogic storage created, remove the CHAP user created during the service deployment from the EqualLogic Group Manager GUI.
- Remove the cluster created in VMware vCenter. If the cluster is no longer needed, remove the cluster from the VMware vCenter GUI.
- In case of Hyper-V removal, perform one of the following methods to remove the created cluster information from the Active Directory server and SCVMM server:

  - (Preferred) Before deleting the service, remove the servers from your domain, and perform the following tasks:

    1. Log in to SCVMM server, set each Host in Maintenance Mode, and then remove the hosts from the cluster.
    2. Remove the hosts and cluster from SCVMM.
    3. Log in to each Host and remove it from the AD Domain.
    4. Delete the service in ASM.

  - If you have already deleted the Service in ASM, perform the following tasks:

    1. Log in to your SCVMM instance, set each Host to Maintenance Mode (error messages will be displayed), and remove the cluster from the SCVMM instance.
    2. Log in to the AD server and perform the following tasks:

       a. Go to the **Active Directory Users and Computers**, click **<Domain>**, and then click **Computers**.

b. Press F5 to refresh and to get the complete list.

c. Delete all of the entries of the computers that are part of the deployment.

– Log in to your DNS server and perform the following tasks:

1. Go to your **Forward Lookup Zones**, click **< Domain >**, and then press F5 to refresh.

2. Delete any stale entries of the IP reservations that were used by the computers and part of your deployment.

**Related Links**

[Decommissioning Services Provisioned by ASM](#)

# Exporting Service Details

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

1. In the **Services** page, perform one of the following actions:
   - To export a service details, select the service, and click **Export to File** in the right pane.
   - To export the details about all the services, click **Export All to File**.
2. Open or save the file.

# Redeploying Failed Service

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

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

# Migrating Servers (Service Mobility)

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

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

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

## Migration Prerequisites

- ASM does not install operating systems on the boot from SAN volume. Therefore, you must install operating system on the servers prior to migration.

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

**Related Links**

> [Migrating Servers](#)

# Migrating Servers

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

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

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

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

# Adding Components to Existing Service Deployments

After a successful service deployment, you can add one or more server, storage, and VM components to an existing service. However, you can only clone the existing component configuration in a service and add a new component. You cannot create a component with a new configuration and add to a service.

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

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

To add components to a service:

1. In the left pane, click **Services**.
   The **Services** page is displayed.
2. Select a service and click **View Details** in the right pane.
   The **Service Details** page is displayed.

3. In the right page, under **Actions**, perform the following steps:
   a. Click **Add Servers** to add a server component to the service.

      > 🖉 NOTE: The **Add Servers** button is displayed only if the service contains a service component.

   b. Click **Add Storage** to add one or more storage components to the service.

      > 🖉 NOTE: The **Add Storage** button is displayed only if the service has a storage component.

   c. Click **Add VM** to add one or more storage components to the service.

      > 🖉 NOTE: The **Add VM** button is displayed only if the service has a storage component.

**Related Links**

[Adding Storage to Existing Service](#)
[Adding Servers to Existing Service](#)
[Adding VMs to Existing Service](#)

## Adding Servers to Existing Service

To add a service to an existing service:

1. On the **Add Server(s)** page, from the **Resource to Duplicate** drop-down list, select the server.
2. In the **# of Instances** box, enter the number of server instances that you want to add to the service, and click **Continue**.
3. In the corresponding **Component Name** boxes, enter the name of the server.
4. Under **OS settings**, enter the name of the host names of the server in the corresponding boxes.
5. Click **Save**.

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

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

- The state of the new server changes from "Available" to "Reserved". Once the deployment starts, the state changes to "Deploying". If the deployment is successful, the state changes to "Deployed". If the deployment is not successful, the state changes to "Error".

## Adding Storage to Existing Service

To add storage components to an existing service:

1. On the **Add Storage** page, from the **Resource to Duplicate** drop-down list, select the storage to clone.
2. In the **# of Instances** box, enter the number of storage instances that you want to add to the service, and click **Continue**.
3. In the corresponding **Component Name** boxes, enter the storage name.
4. Under **Storage Settings**, enter the name of the storage volume in the corresponding boxes.
5. Click **Save**.

## Adding VMs to Existing Service

To add virtual machines to an existing service:

1. On the **Add VM(s)** page, from the **Resource to Duplicate** drop-down list, select the virtual machine to clone.
2. In the **# of Instances** box, enter the number of virtual machine instances that you want to add to the service, and click **Continue**.
3. In the corresponding **Component Name** boxes, enter the name of the virtual machines.
4. Under **Virtual Machine OS Settings**, enter the host name of the virtual machines in the corresponding boxes.
5. Click **Save**.

# 6

# Templates

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

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

- Application
- Virtual Machine
- Cluster
- Server
- Storage

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

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

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

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

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

**NOTE:** A template in Draft state cannot be deployed.

**Template States**

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

**Related Links**
> Manage Templates
> Sample Templates
> Cloning Template
> Deleting Template
> Creating Template
> Editing Template
> Building and Publishing Template
> Importing Template

# Manage Templates

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

The Graphical view displays the following:

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

The Tabular view displays the following information about the template

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

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

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

From this page, you can:

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

**Related Links**
> Sample Templates
> Creating Template
> Editing Template
> Deleting Template
> Cloning Template

## Viewing Template Details

To view more details about a template:

1. In the **Templates** page, select a template.
2. In the right pane, click **View Details**.

   The topology of the components that are part of the template is displayed in the Template Builder page.
3. To view all the component settings, on the Template Builder page, click **View All Settings** in the right pane.

   The **Template Settings** dialog box lists the details about the component configured in the template. For more details about the components settings, see [Component Types](#)

**Related Links**

[Component Types](#)

## Creating Template

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

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

1. In the left pane, click **Templates**.
2. On the **Templates** page, click **Create Template**.

   The **Create Template** dialog box is displayed.
3. Select either **New** or **Clone Existing** option.

   In case of **Clone Existing**, select any existing template that is to be cloned. The components of the selected template are cloned into the new template.
4. Enter a **Template Name**.
5. From the **Template Category** drop-down list, select a template category. To create a new category, select **Create New Category** from the list.
6. Enter **Template Description**. (Optional).
7. To include only specific component type in the template, under **Select which components do you want in your template:**, select the corresponding check boxes to the left of following component types:

   - Application
   - Virtual Machine
   - Cluster
   - Server
   - Storage

8. Click **Save**.

   Instruction appears about creating template. On the instruction page, click the previous or next arrow buttons on the instruction page to read other instructions. If you do not want instructions to be displayed when you login next time, select the **Don't show me this again** check box at the bottom-left corner of the instruction page. To continue building the template using Template Builder page, click **Close**.

**Related Links**

> [Building Template Overview](#)
> [Building and Publishing Template](#)
> [Sample Templates](#)

## Instructions to Create Template

This page provides instructions about creating a template.

You can perform the following actions on this page:

- To view other instructions, click previous or next arrow buttons.

- If you do not want view this instructions again, select the **Don't show this again** check box.

- To close the instruction page and continue building the template, click **Close**.

## Building Template Overview

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

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

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

The following component types can be configured in a template:

- Storage

- Server

- Cluster

- Virtual Machine

- Application

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

On this page, you can:

- Build and Publish a template

- Edit Template name

- Delete a Template

- Import a Template
- Deploy a Service

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

**Related Links**

Building and Publishing Template

## Building and Publishing Template

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

1. If the component is not already selected in the **Create Template** dialog box, to add a component type to your template, select the check box next to a component type, and then click the component icon.

   The corresponding **<component type> component** dialog box is displayed.
2. From the **Select a Component** drop-down list, select the component that you want to add.
3. In the **# of Instances** box, enter the number of component instances that you want to include in a template.
4. Under **Related Components**, select the related components that you want to map with the component instances, and click **Continue**.

   Based on the component type, specific settings and properties appear automatically that are required and can be edited. For more information specific component type settings, see Component Types.
5. Click **Add** to add the component to the Template Builder.
6. Repeat the steps 1 through 5 to add multiple components.
7. After you complete adding components to your template, click **Publish Template**. Publishing a template indicates that a template is ready for deployment.

   If a template is not published, it cannot be deployed and remains in the Draft state until published.
8. After publishing a template, you can use the template to deploy a service in the **Services** page.

**Related Links**

Building Template Overview
Deploy Service
Sample Templates

## Importing Template

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

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

To import a template, perform the following steps:

1. Click **Templates**.
2. **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 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

## Viewing Template Details

To view more details about a template:

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

**Related Links**

    [Component Types](#)

## Deleting Template

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

To delete a template:

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

**Related Links**

    [Sample Templates](#)

## Cloning Template

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

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

## Deploy Service

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

To deploy a service:

1. In the left pane, click **Services**.
   The **Services** page is displayed.
2. On the **Services** page, click **Deploy New Service.**
   The **Deploy Service** dialog box is displayed.
3. In the **Deploy Service** dialog box, perform the following:

   a. From the **Select Template** drop-down list, select the template to deploy a service.

   b. Enter the **Service Name** (required) and **Service Description** (optional) that identifies the service.
4. Click **Deploy Now**.

**Related Links**

Adding Components to Existing Service Deployments
Redeploying Failed Service
Deleting Service
Decommissioning Services Provisioned by ASM

## Decommissioning Services Provisioned by ASM

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

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

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

**Related Links**

Decommissioning Hyper-V Based Storage, Host, and Clusters
Decommissioning VMware Based Storage, Host, and Clusters

### Decommissioning Hyper-V Based Storage, Host, and Clusters

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

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

7. Remove host entries from DNS server.

### Decommissioning VMware Based Storage, Host, and Clusters

To decommission VMware based storage, host, and clusters:

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

## Component Types

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

The following component types are defined in ASM:

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

NOTE: Currently, ASM does not support Switch configuration.

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

**Related Links**

> Storage
> Server
> Cluster
> Virtual Machine
> Application

### Storage

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

The following storage resource types are provisioned in ASM:

- Compellent
- EqualLogic Chap
- NetApp

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

1. In the **Storage Component** dialog box, from the **Select a Component** drop-down list, select one of the storage components:

- **Compellent**
- **EqualLogic**
- **NetApp**

2. Under **Related Components**, select the components that you want to map with the selected storage type. For more information about valid component combinations that can be mapped together in a template, see [Component Combinations in Templates](#)

3. Click **Continue**.

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

   For more information about the storage settings, see [Storage Settings](#)

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

### Storage Settings

| Field Name | Description |
| --- | --- |
| **EqualLogic Chap Storage Settings** | |
| Target EqualLogic Device | Specifies the EqualLogic storage device where the volume is created. |
| Storage Volume | Select the volume in Equallogic. To create a new volume, from the **Storage Volume** drop-down list, select **Create New Volume**. |
| New volume name | Enter the name of the volume in Equallogic. A volume is a logical partition in the EqualLogic storage array. The EqualLogic CHAP users have the access to these storage volumes. More than one chap users can have access to the EqualLogic volume. |
| Storage Pool | Specifies pool name where a volume is. The default storage pool value is *Default*. |
| Storage Size (e.g. 100m, 1g) | Specifies the volume size. |
| Thin Provisioning | Enables thin provisioning on this volume. The possible values are *enable* or *disable*. |
| Snapshot Reserve % | Refers to the amount of space, as a percentage of the volume size, to reserve for a snapshot. |
| Thin Min Reserve % | Sets the minimum reserved size for thin provisioned volume configured as percentage of total volume size. This value cannot be less than 10%. |
| Thin Growth Warning % | Sets the warning threshold percentage for thin-provisioned volume. When the thin-reserve reaches this value, a warning message is displayed. The default value is 60%. |
| Thin Growth Maximum % | Sets the maximum growth percentage for thin volume. When thin-reserve reaches this value, the volume is set to offline. The default value is 80%. |

| Field Name | Description |
|---|---|
| Thin Warning on Threshold % | Specifies whether or not a thin provisioning sends an initiator warning when passing the in-use warning threshold. |
| Thin Warning Hard Threshold % | Specifies whether or not a thin provisioning allows the volume to remain online after reaching the max-growth threshold. |
| Multi-host access of volume | This parameter enables or disables multi-host access on a volume. The possible values are *enable* or *disable*. |
| Authentication | Enables you to select one of the following authentication methods to access the storage volume:<br><br>• **CHAP**<br><br>• **IQN/IP**<br><br>NOTE: For VMware based deployment, you can use IP or Chap authentication. |
| Chap username | Specifies the CHAP username. A valid CHAP username must be less than or equal to 63 alphanumeric characters. The access to CHAP username is limited.<br><br>NOTE: The **Chap username** and **Chap secret** fields are displayed only if authentication type is selected as **Chap**. |
| Chap secret | Specifies the CHAP password. A valid CHAP password must be less than or equal to 254 characters. If the password is not specified, then it is generated automatically. |
| Initiator IQN or IP Addresses | Specifies the IQN or IP addresses that you want to configure on the EqualLogic storage volume to enable access for the IPs or IQNs.<br><br>Enter the comma-separated list containing the IP addresses or IQN addresses. The list should not contain a white space.<br><br>A valid IP address list must be in the format: 172.19.15.2,172.19.15.3,172.19.15.4<br><br>A valid IQN address list must be in the format: iqn.2001-05.com.dellsoftware01,iqn.2001-05.com.dellsoftware02,iqn.2001-05.com.dellsoftware01 |

**Compellent Storage Settings**

| Field Name | Description |
|---|---|
| Target Compellent Device | Specifies the compellent storage device where the volume is created. |
| Storage Volume | Specifies the name of the volume that is to be created or destroyed. |
| Storage Size e.g 100g | Specifies the volume size. Enter the number of 512-byte blocks or the total byte size. To specify a total byte size, use k for kilobytes, m for megabytes, g for gigabytes, or t for terabytes. |
| Boot Volume | Specifies if the mapped volume is designated to be a boot volume. |

| Field Name | Description |
| --- | --- |
| Volume Folder | Specifies the name of an existing volume folder where a volume is to be created. In case the folder does not exist, a new folder is created. |
| Purge Volume | This property indicates that the volume must be purged. If the purge option is not specified, the volume is still visible using the volume show command and contains the status of the Recycled. The possible values are *yes* or *no*. The default value is *yes*. |
| Volume Notes | Specifies the notes for the volume. By default, no notes are included. |
| Replay Profile | Specifies the replay profiles for the volume. |
| Storage Profile Name | Specifies the replay profiles for the volume. |
| Server Notes | Specifies the optional user notes associated with the server. |
| Operating System Type | Specifies the operating system type, which is set in the compellent server object of the compellent storage center. |
| Server Object Folder | Specifies the folder for the server. |
| Server WWN Values | Specifies a globally unique World Wide Name (WWN) for the requested HBA. |
| Port Type | Refers to the transport type for all HBAs being added. This option is required if the manual flag is set. The possible values are *FibreChannel* and *iSCSI*. |
| Manual | This parameter sets an optional flag to configure the requested HBAs before the HBAs are discovered. If the WWN matches a known server port, then this flag is ignored. If this flag is present, then the **Port Type** must also be specified. The possible values are *true* or *false*. |
| Force Map | If the value of this property is defined, it forces mapping, even if the mapping already exists. The possible values are *true* or *false*. |
| Map Read Only | Specifies whether or not a map is read-only. The possible values are *true* or *false*. |
| Single Path Map | Specifies that only a single local port can be used for mapping. If omitted, all local ports are used for mapping. The possible values are *true* and *false*. |
| Configure SAN Switch | Enables the zone configuration on the Brocade FC SAN switch. |
| **NetApp Storage Settings** | |
| Target NetApp * | Specifies the NetApp storage device where the volume will be created. |
| Storage Volume * | Select the volume name on the NetApp array. To create a new volume, from the **Storage Volume** drop-down list, select **Create New Volume**. |

| Field Name | Description |
| --- | --- |
| New volume name | Enter the name of the volume that is to be created or destroyed. The storage volume names created on same aggregate must be unique in a NetApp storage array. |
| Storage Size e.g 100GB * | Specifies the volume size. Enter the number of 512-byte blocks or the total byte size. You can specify the total byte size in the following formats: MB for megabytes, GB for gigabytes, or TB for terabytes. The volume size must be between 20 MB and 999 TB. |
| Aggregate Name * | Specifies the aggregate name on which the volume is created. |
| The space reservation mode | Specifies the type of volume that guarantee the new volume will use. Possible values: **none**, **File**, **Volume**. If any value is not selected, the default volume guarantee type is set to **Volume**. |
| The percentage of space to reserve for snapshots * | Specifies the percentage of space to reserve the snapshots. Default value is 0. |
| Auto increment | Select this check box to enable auto-increment of volume size. By default, auto increment is enabled. |
| Persistent | • In Data ONTAP 7-Mode, the persistent is enabled by default. If it is enabled, modifies the **etc/exports** file to append the rule for a permanent change. (The new rule still takes effect immediately.)<br><br>• In Data ONTAP Cluster-Mode, the export entries are always persistent. Persistent is enabled by default. If persistent is not enabled an error occurs. |
| NFS Target IP | Specifies the interface IP that is used for NFS traffic in your environment. |

## Server

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

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

1. In the **Server Component** dialog box, from the **Select a Component** drop-down list, select a server component.

2. In the **# of Instances,** box, enter the number of the server instances that you want to add.

3. Under **Related Components**, select the components that you want to map with the server components. For more information about valid component combinations that can be mapped together in a template, see [Component Combinations in Templates](#)

4. Click **Continue**.

5. To import an existing server configuration and use it for the server component settings, click **Import from Reference Server**. On the **Select Reference Server** page, select the server from which you want to import the settings, and click **Select**.

6. To import configuration from a server that is part of an existing templates, click **Import from Existing Template**. On the **Select Component** page, select the server under a template, and click **Select**.

7. Specify the settings to be configured on the server components.

For more information about the server settings, see Server Settings

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

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

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

        •   For configuring interface on the Rack Servers, see Configuring Interface on Rack Servers
        •   For configuring interface on the Blade Servers, see Configuring Interface on Blade Servers

9.  Click **Add**.

**Server Settings**

| Target Boot Device | Description |
| --- | --- |
| **Hardware Settings** | |
| Target Boot Device | Specifies the target boot device ( for example: Local Hard Drive or SD card). |
| System Profile | Select the system power and performance profile for the server. |
| User Accessible USB Ports | Enables or disables the user accessible USB ports. |
| Number of Core Processors | Specifies the number of enabled cores per processor. |
| Processor Virtualization Technology | If this is enabled, the additional hardware capabilities provided by virtualization technology are enabled. |
| Logical Processors | Each processor core supports up to two logical processors. If enabled, the BIOS reports all logical processors. If disabled, the BIOS reports only one logical processor per core. |
| Memory Node Interleaving | If the system is configured with matching memory, enables memory node interleaving. If disabled the system supports non-uniform memory architecture memory configurations. |
| Execute Disable | Enables or disable execute disable memory protection |
| Server Pool | Specifies the pool from which servers are selected for the deployment. |
| **OS Settings** | |
| OS Image Type | Refers to the operating system types that are available for deployment, such as Red Hat, Linux, Windows, and Hyper-V. The image type corresponds to the installers that are shipped with ASM for installing a particular type of operating system. For example, you can install Red Hat 6.1, 6.2, 6.3 images and install them all with the Red Hat image type. |

> NOTE: Based on the value selected from the **OS Image Type** drop-down list, the fields related to that OS type are displayed.

| Target Boot Device | Description |
| --- | --- |
| OS Image | Specifies the target repository where the OS image install files are located. The default repositories are ESXi. The additional repositories are shown if the user created them on the ASM appliance. |
| Administrator password | Enter the administrator password that set on the installed OS. |
| Confirm administrator password | Enter to confirm the administrator password. |
| Install EqualLogic MEM | If the value is `True`, install EqualLogic Multipathing Extension Module. |
| Product Key | Specifies the product key to install the OS image on the server. |
| Timezone | Specifies the time zone of the server. |
| NTP Server | Specifies the IP address of the NTP server for time synchronization. |
| Language | Specifies the language to be displayed in the installed operating system. That is, Windows operating system. |
| Keyboard | Specifies the key board language to be used during Windows installation. |
| Domain Name | Specifies the domain name to which you want to add the host. For example, aidev |
| FQ Domain Name | Specifies the Fully Qualified Domain Name (FQDN) to which you want to add the host. For example, aidev.com |
| Domain Admin Username | Specifies the username to access the domain. |
| Domain Admin Password | Specifies the admin password to add the host to the domain. |
| Domain Admin Password Confirm | Enables you to reconfirm the admin password to add the host to the domain. |
| Custom Installation OS Script | Refers to ASM maintained kickstart scripts or **unattend.xml** customer specific scripts to be used as a part of unattend OS install. |

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

## Configuring Interface on Rack Servers

To add a server interface:

1. In the **Server Component** dialog box, select **Rack Server** option under **Targeted Server Type**:
2. For Rack Servers, under Interfaces, click Add New Interface.

3. From the NIC Type, select the NIC type:
   - 2 Port
   - 4 Port
4. Select the **Used for FC** check box, if you want to use the NIC for Fibre Channel.
5. Under specific ports, if you want to partition the port, select the **Do you want to partition?** check box.
6. Enter the following information for each ports or partitions:

   a. Select the vLAN Networks to use for data transmission

   b. Enter the Minimum Bandwidth and maximum bandwidth in percentage.
7. Repeat the steps 4 through 6 for each port.
8. After configuring interfaces, you can configure NIC Teams.
9. Click **Add**.

## Configuring Interface on Blade Servers

1. In the **Server Component** dialog box, under **Fabric Configuration**, select **Blade Server**.
2. To enable the fabrics, select the corresponding check boxes next to **Fabric A**, **Fabric B**, and **Fabric C**.
3. Under **Used for FC**, select the check boxes next to **Fabric B** and **Fabric C** if you want to enable the fabrics for Fibre Channel traffic.
4. From the **NIC Type**, select one of following NIC types:
   - **2 Port**
   - **4 Port**
5. Under **<Port number>**, if you want to partition the port, select the **Do you want to partition?** check box.
6. Perform the following steps for each port and partitions:

   a. In the **Network (vLAN)** column, select the network that you want to configure on the port and partition.

   b. Enter the **Minimum Bandwidth** and **Maximum Bandwidth** in percentage.
7. Repeat the steps 4 through 6 for each port and partition.
8. Click **Add**.

## Importing From Reference Server

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

To import a server configuration, perform the following steps:

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

## Importing From Existing Template

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

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

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

## Cluster

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

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

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

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

## Cluster Component Settings

| Field Name | Description |
| --- | --- |
| **Cluster Settings (Target vCenter)** | |
| Target Hypervisor | Specifies the target VMware vCenter. |
| Data Center Name | Specifies the name of the data center to be created in VMware vCenter. The keyword cluster is not required. |
| New datacenter name | Enables to specify a new data center. |
| Cluster Name | Specifies the name of the cluster to be created in the Data Center. |
| New cluster name | Enables you to specify a new cluster. |
| Cluster HA | Enables or disables highly available cluster. |
| Cluster DRS | Enables or disables distributed resource scheduler. |
| **Cluster Settings (Target Hyper-V)** | |

| Field Name | Description |
|---|---|
| Hypervisor Management Software | Specifies the target SCVMM. |
| Host Group | Specifies the host group that you want to target. |
| New Host Group name | Enables to specify a new host group. Enter the host group in the format: All **hosts\ \<group name\>** |
| Cluster Name | Specifies the name of the cluster. |
| New cluster name | Enables you to specify a new cluster. |
| Cluster IP Address | Specifies the cluster IP address. |

### Virtual Machine

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

After selecting Virtual Machine on the template builder page, perform the following actions:

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

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

    For more information about the virtual machine settings, see [Virtual Machine Settings](#)

### Virtual Machine Settings

| Virtual Machine Settings (Clone vCenter Virtual Machine) | |
|---|---|
| **Field Name** | **Description** |
| **vCenter Virtual Machine** | |
| Virtual Machine OS Settings | |

**Virtual Machine Settings (Clone vCenter Virtual Machine)**

| Field Name | Description |
| --- | --- |
| Administrator password | Specifiy OS administrator password that is set on the installed OS. |
| Confirm administrator password | Enter the password to confirm the administrator password. |
| OS Image | Specifies the target repository where the OS image install files are located. The default repositories are ESXi. The additional repositories will be shown if the user created them on the ASM appliance. |
| OS Image Type | Refers to the operating system types (for example: Red Hat, Linux, Windows and so on.) that are available for deployment. The image type corresponds to the razor "installers" that are shipped with razor and assist razor in installing a particular type of operating system. For example, you can install Red Hat 6.1, 6.2, 6.3 images and install them all with the Red Hat image type. |
| Custom Installation OS script | Refers to ASM maintained kickstart scripts or unattend.xml customer specific scripts to be used as a part of unattend OS install. |
| Virtual Machine Settings | |
| Number of CPUs | Refers to the number of CPUs specified while configuring a Virtual Machine. |
| Virtual Disk Size (GB) | Specifies the size to allocate for virtual machine hard disk. |
| Memory in MB | Refers to the memory in GB specified while configuring a Virtual Machine. |
| Networks | Specifies the networks that will be associated with the virtual machine.  Any networks must be available on the virtualization host for the VM. |

**Virtual Machine Settings (Clone Hyper-V Virtual Machine)**

| Field Name | Description |
| --- | --- |
| Number of CPUs | Refers to the number of CPUs specified while configuring a Virtual Machine. |
| Virtual Disk Size (GB) | Specifies the size to allocate for virtual machine hard disk. |
| Memory in MB | Refers to the memory in GB specified while configuring a Virtual Machine. |
| Networks | Specifies the virtual machine networks to be connected to the virtual machine. |
| Name | Specifies the name of the virtual machine. |
| Source | Specifies the name of the source template. |
| Source Datacenter | Specifies the VMware data center where the source template or virtual machine resides. |

**Virtual Machine Settings (Clone Hyper-V Virtual Machine)**

| Virtual Machine Settings (Clone vCenter Virtual Machine) | |
| --- | --- |
| Field Name | Description |
| Description | Refers to the number of CPUs specified while configuring a Virtual Machine. |
| Name | Specifies the size to allocate for virtual machine hard disk. |
| Template | Specifies the SCVMM virtual machine template name. |
| Path | Specifies the storage path where VM clone will be deployed |
| Networks | Specifies the ASM networks, which will be connected to the virtual machine clone. |
| Block Dynamic Optimization | If it is `True`, the block dynamic optimization will be enabled. Possible values: `True` or `False`. |
| Highly Available | Enables whether the VM is a highly available VM |
| Number of CPUs | Specifies the Number of CPUs to allocate to the virtual machine |
| Memory in MB | Specifies the memory to allocate to the virtual machine |
| Start Action | Selects the action to perform automatically when the virtualization server starts. |
| Start Action | Selects the action to perform when the virtualization server stops. |

### Application

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

ASM provisions multiple applications for deployment.

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

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

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

   See [Application Components Settings](#)
6. Click **Add**.

**Application Component Settings**

| Field Name | Description | Default and Possible Values |
| --- | --- | --- |
| **Mssql 2012** | | |
| Media | Specifies the location of the SQL install image. | Default value: **D:\\** |
| instancename | Specifies a SQL Server instance name for the instance that is being completed. For named instance just enter a user specific name. | Default value: `MSSQLSERVER` |
| features | Specify the list of individual SQL server components to install. | Default values: `SQLENGINE,CONN,SSMS,ADV_SSMS`<br><br>Possible values: `Replication, FullText, DQ, AS, RS, DQC, IS, MDS, BC, BOL, BIDS, DREPLAY_CTLR, DREPLAY_CLT, SNAC_SDT, SDK, LocalDB` |
| sapwd | Specifies the password for SQL Server SA Account. | |
| agtsvcaccount | Specifies the account for the SQL Server Agent service. | Default value: `NT SERVICE \MSSQLSERVER` |
| agtsvcpassword | Specifies the password for SQL Server Agent service account. | Password is not required for NT service accounts. |
| assvcaccount | Specifies the account for the Analysis Services service. | Default value: `NT SERVICE \MSSQLSERVER` |
| assvcpassword | Specifies the password for the Analysis Services service. | Password is not required for NT Service accounts. |
| rssvcaccount | Specifies the startup account for Reporting Services. | Default value: `NT SERVICE \MSSQLSERVER` |
| rssvcpassword | Specifies the password for the startup account for Reporting Services service. | Password is not required for NT Service accounts. |
| sqlsvcaccount | Specifies the startup account for the SQL Server service. | Default value: `NT SERVICE \MSSQLSERVER` |
| sqlsvcpassword | Specifies the password for SQLSVCACCOUNT. | Password is not required for NT Service accounts. |
| instancedir | Specifies a non-default installation directory for shared components. | Default value: **C:\Program Files\Microsoft SQL Server\\** |

| Field Name | Description | Default and Possible Values |
|---|---|---|
| ascollation | Specifies the collation setting for Analysis Services. | Default value: `Latin1_General_CI_AS` |
| sqlcollation | Specifies the collation settings for SQL Server. | Default value: `SQL_Latin1_General_CP1_CI_AS` |
| admin | Specifies the administrator account name | Default value: Administrator |
| netfxsource | Specifies the .Net install file. | |
| **Citrix_xd7** | | |
| Source | Specifies the installation media location | Example, if repository created on appliance repo-store directory. `"//<ASM appliance IP>/razor/ XenDesktop7/x64/ XenDesktop Setup"` |
| SQL Server | If the value is `True`, installs SQL Server component from Citrix installer on the virtual machine to which the component is related. | `Possible values: True` or `False` |
| Delivery Controller | If the value is true, installs Citrix Delivery Controller component from Citrix installer on the virtual machine to which the component is related. | `Possible values: True` or `False` |
| Citrix Studio | If the value is true, installs Citrix Studio component from Citrix installer on the virtual machine to which the component is related. | `Possible values: True` or `False` |
| License Server | If the value is true, installs Citrix License Server component from Citrix installer onto the virtual machine to which the component is related. | `Possible values: True` or `False` |
| Citrix Director | If the value is true, installs Citrix Director component from Citrix installer on the virtual machine to which the component is related. | `Possible values: True` or `False` |
| StoreFront | If the value is true, installs Citrix StoreFront component from Citrix installer on the virtual machine to which the component is related. | `Possible values: True` or `False` |
| **Linux_postinstall** | | |
| Install Packages | Optional. Specify a comma-separated list of yum packages (without spaces) to install. | For example: `openssl,mysql,ntp` |
| Upload Share | Optional. Specifies the share to use for uploading file to server. Share folder must exist. | Default value: **\\myshareserver\folder** |
| Upload File | Optional. Specifies the file to upload from the share that you have specified. | For example: **install.sh** |

| Field Name | Description | Default and Possible Values |
|---|---|---|
| Upload Recursive | Determines whether or not to upload all contents of the directory on the share. (For use in optional upload file/script) | Possible values: `True` or `False` |
| yum_proxy | Optional. Specifies the proxy to use for yum installs. | For example: **http://proxy:80** |
| **Windows_postinstall** | | |
| Share | Optional. Specifies the share to use for uploading file to server. Share folder must be available. | **\\myshareservcer \AppAssureClient** |
| Install Command | Specifies the command to install executable located on the share. | `Agent-Web.exe /silent reboot=never` |
| Upload File | Specifies the file to upload from the share that you have specified. Upload File depends on Share. You must upload file to share. | Possible value: **myfile.bat** |
| Upload Recurse | Determines whether or not to upload all contents of the directory on the share. | Possible value: `True` or `False` |
| Execute File Command | Optional. Specifies the command to execute uploaded file. The command must be used with upload file present. | Possible value: **myfile.bat –u username –p password** |

## Component Combinations in Templates

In the Template Builder and within a template, there are a number of components that can be selected and specified, as discussed in the previous sections. However, only certain combinations of these components can logically be used together. The following table provides information about the valid component combinations supported for template creation. In each vertical column of the table, an X indicates the set of components that can be used together in the same template. For example, reading from the left, a template may contain the following component combinations:

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

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

# Sample Templates

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

**Related Links**

Template – Deploy Citrix XenDesktop for 500 Users
Template – Deploy OS to Hard Drive
Template – Deploy Physical Server and Virtual Machine
Template – Deploy VMs to Cluster
Template – Install ESXi to SD card with FC Storage
Template – Install ESXi to SD Card with iSCSI Storage
Template – Deploy Hyper-V Host with iSCSI Storage
Template – Deploy Hyper-V Cluster with iSCSI Storage
Template – Deploy Hyper-V Cluster with Fibre Channel Storage to SCVMM
Template – Deploy VMWare Cluster with NetApp Storage
Template – Boot from Fibre Channel SAN
Template – Boot from iSCSI SAN
Template – Deploy Virtual Machine Template Clone on Hyper-V Cluster
Template – Deploy Virtual Machine Template Clone on VMWare Cluster

## Template – Deploy Citrix XenDesktop for 500 Users

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

1. In the **Templates** page, select the **Deploy Citrix XenDesktop for 500 Users** and then click the **Clone** button.
2. In the **Create Template** dialog box, enter the **Template Name** and **Template Description** for the template.

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

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

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

      1. Enter the unique names for the **Storage Volume Name** and **Storage Pool**. (Optional)

      2. Update the values of **Storage size**, **Thin Provisioning**, **Snapshot Reserve %**, **Thin Min Reserve %**, **Thin growth Warning %**, **Thin growth Maximum %**, **Thin warning on threshold %**, and **Multi-Host access of volume**.

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

      4. Update the **Chap username** and **Chap secret** text boxes for volume access.

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

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

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

      1. Retain the value of **Target Boot Device** as default value of SD Card.

      2. From the **Server Pool** drop-down list, select the server pool that contains a target server.

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

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

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

      2. Retain the ESXi value as default in the **OS Image Type** drop-down list.

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

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

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

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

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

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

      2. In the **Data Center Name** and **Cluster Name** text boxes, type their corresponding names.

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

   a. Enter the **Administrator password**.

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

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

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

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

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

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

8. To save the settings, click **Save**.

9. To publish the template, click **Publish Template**.

   The template is now ready to be deployed.

## Template — Deploy OS to Hard Drive

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

1. In the **Templates** page, select the **Deploy OS to Hard Drive** template, and then click **Clone** in the right pane.

2. In the **Create Template** dialog box, enter the **Template Name** and **Template Description**.

3. Click **Save**.

4. In the Template Builder, click the server component, click **Edit** in the dialog box that is displayed, and then configure the following settings in the **Server Component** dialog box.

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

6. Under **Hardware Settings**, perform the following:

   a. From the **Target Boot Device** drop-down list, select the corresponding target boot device.

   b. From the **Server Pool** drop-down list, select the corresponding server pool.

7. Under **OS Settings**, perform the following:

    a. To select the administrator password that you want to configure on the deployed OS, in the **Administrator password** box, type the administrator password.

    b. In the **Confirm administrator password** box, retype the password again to confirm.

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

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

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

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

9. To save the settings, click **Save**.

10. To publish the template, click **Publish Template**.

    The template is now ready to be deployed.

## Template – Deploy Physical Server and Virtual Machine

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

1. On the **Templates** page, select the **Deploy Physical Server and Virtual Machine**, and then click **Clone** in the right pane.

2. In the **Create Template** dialog box, enter the **Template Name** and **Template Description**.

3. In the Template Builder, click the server component, click **Edit** in the dialog box that is displayed, and then in the **Server Component** dialog box, perform the following configurations:

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

    b. Under **Hardware Settings**, from the **Server Pool** drop-down list, select the corresponding server pool.

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

4. Under **OS Settings**, perform the following:

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

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

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

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

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

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

8. Under **Related Components**, select corresponding components. (Optional)

9. Under **Cluster Settings**, perform the following:

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

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

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

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

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

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

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

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

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

11. To save the settings, click **Save**.

12. To publish the template, click **Publish Template**.

    The template is now ready to be deployed.

## Template — Deploy VMs to Cluster

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

1. In the **Templates** page, select the **Deploy VMs to Cluster** template, and then click **Clone** in the right pane.

2. In the **Create Template** dialog box, enter the **Template Name** and **Template Description** for the template.

3. Click **Save**.

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

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

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

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

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

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

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

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

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

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

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

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

6. To save the settings, click **Save**.

7. To publish the template, click **Publish Template**.

   The template is now ready to be deployed.

## Template — Install ESXi to SD card with FC Storage

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

1. In the **Templates** page, select the **Install ESXi to SD card with FC Storage** template, and then click **Clone**.

2. In the **Create Template** dialog box, enter the **Template Name** and **Template Description** for the template.

3. Click **Save**.

4. In the Template Builder, select the storage component, click **Edit** in the box that is displayed, and then configure the following settings in the **Storage Component** dialog box.

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

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

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

      2. in **Storage Size e.g 100GB** text box, enter storage size.

      3. Do not modify the **Boot Volume** settings.

      4. In the **Volume Folder**, **Volume notes**, **Replay Profile**, **Storage Profile Name**, and **Server Notes** text boxes, type the details. (Optional)

      5. In the **Server Object Name** box, type a server object name.

      6. From the **Operating System Name** drop-down list, select either VMware ESX 5.1 or 5.5.

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

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

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

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

      1. Retain the value of **Target Boot Device** as default value of SD Card.

      2. From the **Server Pool** drop-down list, select corresponding server pool.

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

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

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

      2. Retain the value ESXi as default in the **OS Image Type** drop-down list.

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

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

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

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

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

7. To save the settings, click **Save**.

8. To publish the template, click **Publish Template**.

   The template is now ready to be deployed.

## Template — Install ESXi to SD Card with iSCSI Storage

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

1. In the Templates page, select the **Install ESXi to SD Card with iSCSI Storage** template, and click **Edit** in the right pane.

2. In the **Create Template** dialog box, enter the **Template Name** and **Template Description** for the template.

3. Click **Save**.

4. In the Template Builder, select the EqualLogic storage component, click **Edit** in the box that is displayed, and then configure the following settings in the **Storage Component** dialog box.

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

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

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

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

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

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

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

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

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

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

      1. Retain the value of **Target Boot Device** as default value of SD Card.

      2. From the **Server Pool** drop-down list, select corresponding server pool.

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

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

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

      2. Retain the ESXi value as default in the **OS Image Type** drop-down list.

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

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

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

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

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

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

9. To save the settings, click **Save**.

10. To publish the template, click **Publish Template**.

    The template is now ready to be deployed.

## Template — Deploy Hyper-V Host with iSCSI Storage

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

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

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

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

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

      1. From the **Target EqualLogic** drop-down list, select the Target EqualLogic iSCSI array.

      2. In the **Storage Volume Name** box, enter a unique name for the storage volume, if required.

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

      3. Verify the values for **Storage Pool**, **Thin Provisioning**, **Snapshot Reserve %, Thin Min Reserve %**, **Thin growth Warning %**, **Thin growth Maximum %**, **Thin warning on threshold %**, **Thin warning on hard threshold %**, and **Multi-Host access of volume**.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   m. Click **Save**.

**6.** Click **Publish Template**.

This template is now ready to be deployed.

## Template — Deploy Hyper-V Cluster with iSCSI Storage

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

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

**1.** On the **Templates** page, select the **Deploy Hyper-V Cluster with iSCSI Storage** template, and click **Clone**.

**2.** In the **Create Template** dialog box, enter a name, description, category for the template, and click **Save**.

**3.** On the **Template Builder** page, click each storage components, click **Edit** in the box that is displayed, and configure the following settings in the **Storage Component** dialog box.

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

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

        1. Select your **Target EqualLogic** iSCSI array.

        2. Enter the **Storage Volume Name** if required.

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

    c. Verify the values for **Storage Pool**, **Thin Provisioning**, **Snapshot Reserve %, Thin Min Reserve %**, **Thin growth Warning %**, **Thin growth Maximum %**, **Thin warning on threshold %**, **Thin warning on hard threshold %**, and **Multi-Host access of volume**.

    d. Click **Save**.

4. On the **Template Builder** page, click each server components in the swim lane, and configure the following settings for both the servers:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

    e. Click **Save**.

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

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

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

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

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

    e. Click **Save**.

6. Click **Publish Template**.

This template is now ready to be deployed.

**Related Links**

    Template – Deploy Citrix XenDesktop for 500 Users
    Template – Deploy OS to Hard Drive
    Template – Deploy Physical Server and Virtual Machine

## Template – Deploy Hyper-V Cluster with Fibre Channel Storage to SCVMM

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

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

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

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

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

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

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

4. Click **Save**.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6. Click **Save**.

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

   a. From the **Hypervisor Management Software** drop-down list, make sure that you select your target SCVMM.

   b. From the **Host Group** drop-down list, select an existing host group, or in the **New host group name** box and enter the name of the host group that you want to create.

   c. From the **Cluster Name** drop-down list, select **New Cluster** and then in the **New cluster name** box, enter an updated name for the cluster that will be created in SCVMM.

8. Click **Save**.

9. Click **Publish Template**.

This template is now ready to be deployed.

## Template — Deploy VMWare Cluster with NetApp Storage

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

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

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

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

   b. From the **Target NetApp** drop-down list, select the target NetApp Storage.

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

   d. From the **Aggregate Name**, select the aggregate name that is used in your NetApp storage.

   e. From the **NFS Target IP**, select the target NFS IP that will be used.

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

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

   b. Retain the default selection of **SD Card** for **Target Boot Device**.

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

   d. Edit the **Administrator Password** for the ESXi host.

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

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

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

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

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

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

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

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

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

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

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

6. Click **Save**.

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

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

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

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

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

   This template is now ready to be deployed.

## Template — Boot from Fibre Channel SAN

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

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

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

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

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

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

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

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

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

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

   c. Select the appropriate workload networks.

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

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

6. Click **Save**.

7. Click **Publish Template**.

   This template is now ready to be deployed.

## Template — Boot from iSCSI SAN

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   This template is now ready to be deployed.

## Template — Deploy Virtual Machine Template Clone on Hyper-V Cluster

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

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

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

1. On the **Templates** page, select the **Deploy Virtual Machine Template Clone on Hyper-V Cluster** template, and click **Clone** in the right pane.
2. In the **Create Template** dialog box, enter a name, category, and description for the template, select the cluster and virtual machine components, and click **Save**.

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

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

   b. From the **Host Group** and **Cluster Name** drop-down lists, select the host group and cluster name on which virtual machine clone will be deployed.

4. Click **Save**.

5. On the **Template Builder** page, click the virtual machine component, click **Edit** in the dialog box that is displayed, and then configure the following settings for the virtual machine in the **Virtual Machine Component** dialog box:

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

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

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

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

      ✎ **NOTE:** Any network selected must be enabled and available on the SCVMM hosts/clusters where the virtual machine will be deployed.

6. Click **Save**.

7. Click **Publish Template**.

   This template is now ready to be deployed.

## Template — Deploy Virtual Machine Template Clone on VMWare Cluster

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

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

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

1. On the **Templates** page, select the **Deploy Virtual Machine Template Clone on VMWare Cluster** template, and click **Clone** in the right pane.

2. In the **Create Template** dialog box, enter a name, category, and description for the template, select the cluster and virtual machine components, and click **Save**.

3. On the **Template Builder** page, click the VMWare Cluster component, click **Edit** on the dialog box that is displayed, and then configure the following settings in the **Cluster Component** dialog box:.

   a. From the **Target Virtual Machine Manager** drop-down list, select the target Virtual Machine Manager instance where the clone will be created

   b. From the **Data Center Name** drop-down list, select the data center on which virtual machine will be deployed.

   c. From the **Cluster Name** drop-down list, select the cluster on which virtual machine will be deployed.

4. Click **Save**.

5.  On the **Template Builder** page, click the virtual machine component, click **Edit** in the dialog box that is displayed, and then configure the following settings for the virtual machine in the **Virtual Machine Component** dialog box:

    a.  Modify the **Component Name** of the virtual machine, as required.

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

        ✎ **NOTE:** Any network selected must be enabled and available on the SCVMM hosts/clusters where the virtual machine will be deployed.

    c.  Update the name for the virtual machine clone.

    d.  Select the type of clone to be created, if the source is the virtual machine or if the source is a virtual machine template.

    e.  From the **Source** drop-down list, select a valid VMWare virtual machine template or virtual machine that has been prepped according to the instruction provided in the *Active System Manager version 6 Quick Installation Guide*.

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

    f.  Select the datacenter where the source template is located.

6.  Click **Save**.

7.  Click **Publish Template**.

    This template is now ready to be deployed.

## Template — Deploy SQL Server 2012

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

To configure ASM virtual appliance:

1.  Log in to ASM virtual appliance as delladmin. The default delladmin credentials are `delladmin`/ `delladmin`.

2.  You must copy Microsoft SQL Server 2012 ISO to the **/var/lib/razor/repo-store/** directory.

3.  Unpack Microsoft SQL Server 2012 ISO into CIFs share on the virtual appliance. To perform this task, run the following commands: **cd /var/lib/razor/repo-store mount -o loop <SQL2012>.iso/mntrsync - a /mnt/ /var/lib/razor/repo-store/ SQL2012umount /mntrm SQL2012.iso**

4.  On the ASM home page, in the left pane, click **Templates**, select the **Deploy SQL Server 2012** template, and then click **Clone**.

5.  In the **Create Template** dialog box, enter a name, category, and description. Click **Save**.

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

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

      1. From the **Authentication** drop- down list, select the one of the following authentication types based on your environment: **IQN/IP** or **CHAP**.

      2. If you have selected the authentication type as **CHAP**, enter the **Chap username** and **Chap secret** for the storage volume

      3. If you have selected the authentication type as **IQN/IP**, enter the **Initiator IQN** or **IP address** for the storage volume.

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

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

   c. Click **Save**.

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

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

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

   c. Click **Save**.

8. On the Template Builder page, click the cluster component, and configure the following:

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

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

   c. Click **Save**.

9. On the Template Builder page, click the virtual machine, and configure the following:

   a. Enter the **Administrator password**.

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

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

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

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

   f. Click **Save**.

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

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

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

    c. Click **Save**.

11. Click **Publish Template**.

    This template is now ready to be deployed.

# Additional Template Information

This section provides additional details, including prerequisites, for creating or deploying certain types of templates.

## Deploying ESXi Cluster for SAN Applications

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

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

**Related Links**

Creating Template for ESXi Cluster Deployment
Deploying Service on ESXi Clusters
Cleaning Up ESXi Cluster Deployments
ESXi Cluster Deployment Perquisites

### ESXi Cluster Deployment Perquisites

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

| Specification | Prerequisite |
| --- | --- |
| Chassis IOM Configuration (if blade use case) | Make sure that the SAN IOM is in access gateway mode. |
| Managed Rack or Blade Servers Configuration | Make sure that the QLogic FC Adapters installed in any slot for rack servers or fabric B or C for blade servers. ASM will query for WWPN values on a QLogic QME or QLE 2662 or 2572 adapter. |
| Brocade Switch Configuration | • Create fault domain on Brocade switches for Compellent.<br>• Create both physical and logical ports of the Compellent array.<br>• Make sure active zone set is configured on the Brocade SAN switches. |

| Specification | Prerequisite |
|---|---|
| Compellent Storage Configuration | Must be configured |
| Resource Discovery | Make sure the following resources are discovered in ASM. |

- FC Servers for Deployment
- FC SAN Brocade Switch
- FC IOMs (Optional)
- Dell Compellent Storage
- VMware vCenter

### Creating Template for ESXi Cluster Deployment

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

- In the **Template Builder** page, add the following resources by clicking the corresponding components icons.

  - Storage

  - Server

  - Cluster

- To configure Brocade switches, perform the following actions:

  a. In the Storage, click the corresponding storage component icon.

  b. In the **Storage Component** pane, under **Compellent Storage Settings**, set the value as `true` for **Configure SAN Flag** parameter.

- The parameter **iSCSI network** is not required when deploying Fibre Channel storage. If this setting is included, it will be ignored.

**Related Links**

Creating Template
Building Template Overview
Building and Publishing Template

### Deploying Service on ESXi Clusters

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

ASM performs the following actions when you deploy this service:

- Identifies the necessary servers from the FC server pool specified.

- Boots the server when if it is turned on and verifies the FC connectivity.

- Creates the storage volume and server objects that contain the WWPNs on Compellent storage. ASM creates the storage volume and server objects with the names specified in the template.

- If **Configure SAN Switch** parameter is set to true, ASM performs the following actions:

- Identifies the fault domain of the Compellent storage created on the Brocade switches.
- Configures the Brocade switch by creating a zone for the server including the WWPN of the FC adapters and the Compellent storage. The zones will be added to the active zone set.
- Maps the server object to the Compellent volume.
- Installs ESXi, creates virtual networking based on the template, and creates and formats the VMFS data store for the attached Compellent volume and configures multipathing settings.

**Related Links**

[Creating Template](#)
[Building Template Overview](#)
[Building and Publishing Template](#)
[Deploy Service](#)

## Cleaning Up ESXi Cluster Deployments

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

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

# 7

# Resources

The Chassis, servers, switches, storage groups, VMware vCenters, and System Center Virtual Machine Managers (SCVMM) that you can manage using ASM are called resources.

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

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

**Related Links**

## Understanding All Resources Tab

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

- State in which the resource exists. For example, Available, Deployed, Pending, Error, and so on.

  > NOTE: The state column displays the last discovery state of the resources. To manually run the inventory operation on a resource and update ASM with the latest resource details, click a resource, and then click **Run Inventory** in the **Details** pane.

- IP address of the resource. (Click the IP address of a Dell resource to open the Element Manager.)
- Resource ID that uniquely identifies a resource in the form of service tag, host name, or FQDN based on the resource types.
- Manufacturer name. For example, Dell, Cisco, VMware, and so on.
- Resource model. For example, M620, M1000e, PowerEdge VRTX, and so on.
- Resource type. For example, Chassis, Blade Server, EqualLogic Storage Group, VMware vCenter, and so on.

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**
- **Hypervisor Management Software**

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

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

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

**Related Links**

> [Discovering Resources](#)

### Discovering Resources

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

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

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

To discover the resources:

1. On the **Welcome** page of the **Discover Resources** wizard, read the instructions, and click **Next**.
2. On the **Identify Resources** page, click **Add Resource Type**, and perform the following steps:

   a. Select the resource type.
   b. Type the IP address range of the resources that you want to discover.
   c. To manage or unmanage the resources that you discover, select **Managed** or **Unmanaged**.
   d. Select or create a new credentials to discover resource types.

3. To discover multiple resources with different IP address ranges, repeat the step 2, and then click **Next**.

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

4. On the **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

1. On the **Identify Resources** page, click **Add Resource Type**, and perform the following steps:

   a. From the **Resource Type** drop-down list, select one of the following resource types:

      - **All**
      - **Server**
      - **Storage**
      - **Switch**
      - **vCenter**
      - **SCVMM**
      - **Chassis**

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

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

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

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

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

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

2. To discover a different resource type and resources of same type with different credentials, repeat the step 1.

3. Click **Next** to discover and collect the inventory data from the resources.

### 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 ASM, perform the following steps:

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

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

> ✎ **NOTE:** You cannot remove a chassis that is in any Pending state.

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

## Updating Resource Inventory

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

1. In the left pane, click **Resources**.
2. On the **Resources** page, click the **All Resources** tab.
3. From the list of resources, click a resource, and in the **Details** pane, click **Run Inventory**.
   An inventory job is scheduled, the resource state changes to Pending. When the inventory is complete, the resource state changes to Available. See ASM logs to view the start time and end time of the resource inventory operation.

## Managing and Unmanaging Resources

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

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

## Viewing Resource Details

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 7.6 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](#)
[GUID-192C4803-48EA-4D8F-BA0D-2D61821E0601](#)
[Viewing VMware vCenter Details](#)

### Resource Operational State

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

| State | Description |
| --- | --- |
| Available | Resource is available for deployment. |
| Deploying | Resource is in the process of being deployed in a service. |
| Deployed | Resource is deployed in a service. |
| Pending | One or more of the following tasks are in progress:<br>• Discovering resource.<br>• Determining resource details, including firmware version.<br>• Applying template to the resource.<br>• Updating firmware.<br>• Removing resource from ASM inventory. |
| Error | Service deployment is failed. |
| Reserved | Resource is reserved by a service prior to a pending deployment. |
| Unmanaged | Resource is not managed by ASM. |

### Viewing Chassis Details

1. In the left pane, click **Resources**.

   The **Resources** page is displayed.
2. In the **All Resources** tab, click a chassis from the list of resources to view the details.

   The **Details** pane in the right displays the basic information about the Chassis, such as Power State, Management IP, Chassis Name, Service Tag, and Location.

3. To view the detailed information about the Chassis, in the **Details** pane, click **View Details**.
   The **Chassis Details** page displays the detailed information about the Chassis in the following tabs.

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

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

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

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

### Viewing Blade or Rack Server Details

1. In the left pane, click **Resources**.
   The **Resources** page is displayed.
2. In the **All Resources** tab, click a blade server or rack server from the resources list to view the details
   The **Details** pane in the right displays the basic information about the blade servers, such as Power State, Management IP, Host name, Service Tag, Location, OS, DNS DRAC Name, Processors, and Memory.
3. In the **Details** pane, click **View Details**.
   The **Blade Server Details** page displays the detailed information about the server in the following tabs.

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

   - **Summary**
   - **Network Interfaces**
   - **Firmware Revisions**
   - **CPUs**

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

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

### Viewing VMware vCenter Details

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

### Viewing SCVMM Details

1. In the left pane, click **Resources**.

   The **Resources** page is displayed.

2. In the **All Resources** tab, click a System Center Virtual Machine Manager (SCVMM) from the resource list to view the details.

   The **Details** pane in the right displays the following basic information about the SCVMM:

   - Power State
   - Host Groups
   - Clusters
   - Hosts
   - Virtual Machines

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

### Viewing Storage Group Details

1. In the left pane, click **Resources**.

   The **Resources** page is displayed.

2. In the **All Resources** tab, click a storage group from the resources list to view the details.

   The **Details** pane in the right displays the basic information about the storage group, such as System Status, Management IP, Storage Center Name, Group Members, Volumes, Replay Profile, Free Group Space. For NetApp storage type, displays the Storage Name, Available Storage, Aggregates, Volumes, and Disks.

3. In the **Details** pane, click **View Details**.

   The **Storage Group** details page displays detailed information about storage group in the following tabs:

   - Summary
   - Volumes

   > **NOTE:** In ASM 7.6 release, the detailed information can be viewed only for Dell Resources.

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

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

### Opening the iDRAC Remote Console

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

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

1. In the left pane, click **Resources**.
2. On the **Resources** page, click the **All Resources** tab.
3. Click a server.
4. In the **Details** pane, click **View Details**.

5. In the **Summary** tab, under **Actions** in the right, click **Launch iDRAC GUI**.

### Opening the CMC Remote Console

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

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

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

# Understanding Server Pools

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

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

- 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.

# 8

# 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 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

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

You can view the following information:

- Severity

    - ❌ — Indicates the fatal error occurred while communicating with a managed resource; corrective action is immediately required.

    - ⚠️ — Indicates that the resource is in a state that requires corrective action, but does not impact overall system health. For example, a discovered resource is not supported.

    - ℹ️ — Indicates general information about system health or activity.

    - ✅ — Indicates that the component is working as expected.

- Category

    - Security — Indicates the authentication failures, operations on ASM users, operations on credentials

- – Appliance Configuration — Indicates the initial setup, appliance settings, backup and restore
- – Template Configuration — Indicates the operations on Service Templates
- – Network Configuration — Indicates the operations on networks, pools for MAC/IQN/WWPN/WWNN
- – Infrastructure or Hardware Configuration — Indicates the hardware discovery, inventory
- – Infrastructure or Hardware Monitoring — Indicates the hardware health
- – Deployment — Indicates the Service template deployment operations
- – Licensing — Indicates the license updates and expirations
- – Miscellaneous — Indicates all other issues
- Description — Displays brief summary of activity
- Date and Time — Indicates the time when activity occurred and time is displayed using the client machine time zone.  In case of logs, the time captured when the message is logged is based on the appliance time.
- User — Indicates user name from which activity originated

On this page, you can:

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

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

**Related Links**

## Exporting All Log Entries

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

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

## Purging Log Entries

You can delete log entries based on date and severity.

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

   ⚠ **CAUTION: If you do not select a date, then ALL entries with the selected severity level(s) are deleted.**

4.  To delete entries by severity level, select **Information**, **Warning**, and **Critical.**

    ⚠ **CAUTION: If you do not select a severity level, then ALL entries older than the selected date are deleted.**

5.  Click **Apply.**

    📝 NOTE: You must select either a date or at least one severity level.

# Backup and Restore

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

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

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

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

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

On this page, you can:

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

**Related Links**

> [Backup Now](#)
> [Restore Now](#)
> [Editing Backup Settings and Details](#)
> [Editing Automatically Scheduled Backups](#)

## Backup Details

ASM backup file includes following information:

*   Activity logs
*   Credentials
*   Deployments
*   Resource inventory and status

- Events
- Identity Pools
- Initial setup
- IP addresses
- Jobs
- Licensing
- Networks
- Templates
- Users and roles
- Resource Module configuration files

## Editing Backup Settings and Details

1. In the left pane, click **Settings**, and then click **Backup and Restore**.
2. On the **Backup and Restore** page, under **Settings and Details** section, click **Edit**.
3. Optionally, to indicate the network share location where the backup file will be saved, type a backup directory path in the **Backup Directory Path** box. Use one of the following formats:
   - NFS – **host:/share/**
   - CIFS – **\\host\share\**

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

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

## Editing Automatically Scheduled Backups

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

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

3. Select one of the following options:

   - To use the general settings that are applied to all backup files, select **Use Backup Directory Path and Encryption Password from Settings and Details**.

   - To use custom settings:

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

        – NFS – **host:/share/**

        – CIFS – **\\host\share\**

     2. Optionally, type a username and password in the **Backup Directory User Name** and **Backup Directory Password** boxes, if they are required to access the location you typed in the earlier task.

     3. In the **Encryption Password** box, type a password that is required to open the backup file, and verify the encryption password by typing the password in the **Confirm Encryption Password** box.

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

4. Click **Backup Now**.

## Restore Now

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

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

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

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

The restore process is started.

# Credentials Management

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

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

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

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

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

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

- Name of the user who created and modified the credential.

- Date and time that the credential was created and last modified.

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

- Create New Credentials
- Edit Existing Credentials
- Delete Existing Credentials

**Related Links**
>   [Creating Credentials](#)
>   [Editing Credentials](#)
>   [Deleting Credentials](#)

## Creating Credentials

To create new credentials:

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

5. In the **User Name** field, type the user name for the credential.

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

6. In the **Password** and the **Confirm Password** boxes, type the password for the credential.

> **NOTE:** For valid user name and password formats, see the iDRAC, CMC, I/O module, or see the storage third-party documentation.

7. Optionally, for VMware vCenter and SCVMM, in the **Domain** box, enter the domain ID.
8. Optionally, for switch credentials:
   a. Under **Protocol**, click one of the following connection protocols used to access the resource from remote.
      - **Telnet**
      - **SSH**
   b. Under **SNMP Configuration**, in the **SNMP v2 Community String** box, type the SNMP v2 community string required to access the resource.
9. To save the credential, click **Save**.

**Related Links**

[Editing Credentials](#)
[Deleting Credentials](#)

## Editing Credentials

To edit a credential:

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

## Deleting Credentials

To delete a credential:

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

**Related Links**

[Creating Credentials](#)
[Editing Credentials](#)

# Networks

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

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

Additionally, make sure that the following network prerequisites are met:

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

**Related Links**

Networking
Defining or Editing Existing Network
Deleting a Network

## Networking

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

- Name
- Description
- VLAN ID
- Network Type

From this page, you can:

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

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

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

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

**Related Links**

Network Types
Defining or Editing Existing Network
Deleting a Network

### Defining or Editing Existing Network

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

To define or edit an existing network:

1. In the left pane, click **Settings**, and then click **Networks**.
   The **Networks** page is displayed.
2. Perform one of the following:
   - To define a network, click **Define**.

     The **Define Network** page is displayed.
   - To edit an existing network, select the network that you want to modify, and click **Edit**. The **Edit Network** page is displayed.
3. In the **Name** field, type the name of the network.
4. Optionally, in the **Description** field, type a description for the network.
5. From the **Network Type** drop-down list, select one of the following network types. For more information about network types, see Network Types.
   - Private LAN
   - Public LAN
   - SAN [Software iSCSI]
   - SAN [FCoE]
   - Hypervisor Management
   - Hypervisor Migration
   - Hypervisor Cluster Private
   - PXE
   - Fileshare

   **NOTE:** The virtual MAC identity that ASM assigns to the NIC depends on the network type selected when adding a network.
   - For a LAN network type, a virtual MAC address is assigned to the server.
   - For an iSCSI network type, a virtual iSCSI MAC address is assigned to the server.
   - For an FCoE network type, a virtual FIP MAC address is assigned to the server.
6. In the **VLAN ID** field, type the VLAN ID between 1 and 4094.

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

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

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

   📝 **NOTE:** Currently, stating IP addressing is not supported for SAN [FCoE] network types.

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

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

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

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

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

**Related Links**

[Network Types](#)
[Deleting a Network](#)

## Network Types

Using ASM, you can manage the following network types.

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

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

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

## VLAN ID

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

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

### Deleting a Network

**NOTE:** You should not delete a network that is referenced in a template. This will affect the services that will be deployed using this template.

To delete a network:

1. In the left pane, click **Settings**, and then click **Networks**.
   The **Networks** page is displayed.
2. Click the network that you want to delete, and then click **Delete**.
3. Click **OK** when the confirmation message is displayed.

**Related Links**

   [Network Types](#)
   [Network Types](#)
   [Defining or Editing Existing Network](#)

# Users

The **Users** page allows you to manage the users within ASM. You can create a new user, or edit, delete, enable, disable or import existing users from Active Directory.

The **Users** page displays the following information about users:

- User Name
- Domain
- Role
- Last Name
- First Name
- State (*Enabled* or *Disabled*)

On this page, you can:

- Edit or delete an existing user.
- Create local user.
- Enable or disable a user account.
- Import Active Directory Users.

Additionally, you can click on the specific user account to view the following user related information:

- Email
- Phone
- Directory Services

**NOTE:** You can also refresh the information on the page. To sort the users list based on the entries in a column, click the arrow next the column header.

## Creating a User

The Create option allows you to create a new ASM user. Enter the following information to create a new user.

1.  On the left pane, click **Settings**, and then click **Users**.
2.  On the **Users** page, click **Create**.
3.  Enter a unique **User Name** to identify the user account.
4.  Enter a **Password** that a user will enter to access ASM. Confirm the password.

    **NOTE:** The password length must be between 8-32 characters and must include at least one number, one capital letter, one lowercase letter, and one special character.

5.  Enter the user's **First Name** and **Last Name**.
6.  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.  In the left pane, click **Settings** and then click **Users**.
2.  On the **Users** page, select one or more user accounts to delete.
3.  Click **Delete**.
    Click **Yes** in the warning message to delete the account(s).

## Editing a User

The Edit option allows you to edit an ASM user profile. Perform the following tasks to edit a user profile:

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

**Related Links**
>   Users
>   Creating a User
>   Deleting a User
>   Enabling or Disabling Users

## Enabling or Disabling Users

The **Enable** option allows you to change the user account state to *Enabled* and the **Disable** option allows you to change the user account state to *Disabled*. Perform the steps below to enable or disable the user account state:

1. In the left pane, click **Settings**, and then click **Users**.
2. On the **Users** page, select one or more user accounts to enable/disable.
3. In the menu, click **Enable** or **Disable**, to update the State to Enabled or Disabled, as selected.

    📝 **NOTE:** For an already *Enabled* user account **State**, the **Enable** option in the menu is deactivated, and for an already *Disabled* user account **State**, the **Disable** option in the menu is deactivated.

## Directory Services

The Directory Services functionality allows you to create Directory Service that ASM can access for importing remote users.

On this page, you can:

- Create a Directory Service.
- Delete a Directory Service.
- Edit a Directory Service.

### Directory Services

The **Directory Services** option allows you to add, edit or delete an Active Directory using the **Directory Services** functionality. ASM can access these active directories to import users.

📝 **NOTE:** An Active Directory user is authenticated against the specific Active Directory Domain that a user belongs to.

📝 **NOTE:** While logging into the ASM software, the Active Directory user is required to first enter the directory name that a user belongs to, followed by the username, for example: domain/username.

The **Directory Services** page displays the following information about the ASM active directories:

- Host IP address
- Name
- Directory Type

From this screen, you can:

- Add a directory service.
- Edit or Delete an existing directory service.

**Related Links**

Deleting a Directory Service
Editing a Directory Service

## Adding a Directory Service

To add a Directory Service, configure the following:

- **Connection Settings**
- **Attribute Settings**

## Connection Settings

1. In the left pane, click **Settings**, and then click **Users**.
2. In the **Directory Services** tab, click **Create**.
3. Select the directory service type from the **Type of Directory Service** drop-down list.
4. Enter the directory service name in the **Name** box.
5. Enter the **User Name**, **Password**, **Host**, **Port** and **Protocol** (*Plain* or *SSL*) of the Active Directory that is to be added to ASM.

   > NOTE: The default Windows port is 389, but refer to your Active Directory configuration for the specific port used for your Active Directory. Currently, the only format supported for **User Name** is <user name>@<domain.com >.

6. Click **Next**.

**Related Links**

Attribute Settings
Summary
Importing Users
Connection Settings Matrix
Attribute Settings Matrix

## Connection Settings Matrix

| Field Name | Description |
| --- | --- |
| Type Of Directory Service | Refers to the type of directory service (currently available, Microsoft Active Directory). |
| Name | Refers to the Active Directory (AD) configuration name as added in ASM. For example: mydomain |
| User Name | Refers to the AD account that has privileges to search for users. The account name must be entered using the User Principle Name format. For example: administrator@mydomain.com |
| Password | Refers to the AD server password for the account in the **User Name** box. |
| Host | Refers to the AD server FQDN host name or IP address. For example: 192.168.0.5 |
| Port | Refers to the AD server port. For example: 389 |
| Protocol | Refers to the protocol type as Plain or SSL.<br><br>For example: Plain |

## Attribute Settings

The **Attribute Settings** allows you to perform the attribute settings required for adding an Active Directory.

1. Enter the **Base DN**, **Filter**, **Username Attribute**, **First Name**, **Attribute**, **Last Name Attribute**, and the **Email Attribute** of the Active Directory that is to be added to ASM.
2. Click **Next**.

**Related Links**

## 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.<br><br>For example: CN=Users,DC=mydomain,Dc=com |
| Filter | Refers to the filters that enable you to define search criteria. For example: objectClass=* |
| User Name Attribute | Refers to the Active Directory record attribute that represents the User Name attribute. This attribute is mapped to ASM User Name attribute. For example: sAMAccountName |
| First Name Attribute | Refers to the Active Directory record attribute that represents First Name. This attribute is mapped to ASM First Name attribute. For example: givenName |
| Last Name Attribute | Refers to the Active Directory record attribute that represents the Last Name of the user. This attribute is mapped to ASM Last Name attribute. For example: sn |
| Email Attribute | Refers to the Active Directory record attribute that represents the Email of the user. This attribute is mapped to ASM Email attribute. For example: mail |

## Summary

The **Summary** option allows you to verify the entered connection and attribute settings before committing the settings. Perform the required steps as mentioned below:

1. To change the **Connection Settings** or the **Attribute Settings**, click **Back**.
2. To create the directory services with the existing settings, click **Save**.

**Related Links**

### Editing a Directory Service

The **Edit** option allows you to edit the existing directory settings. Perform the following steps to edit the active directory settings:

1. In the left menu, click **Settings**, and the click **Users**.
2. In the **Directory Services** check box, select a single directory service to be edited by checking the required service directory check box.
3. Edit the **Connection settings**, as necessary.
4. Edit the **Attribute Settings**, as necessary.
5. Review the **Summary** and edit settings. (Optional).
6. Click **Save** to update the edited settings.

**Related Links**

[Deleting a Directory Service](#)

### Deleting a Directory Service

The **Delete** option allows you to delete a directory service. Perform the following steps to delete a directory service:

1. In the left pane, click **Settings**, and then click **Users**.
2. In the **Directory Services** tab, select a single or multiple directory services to be deleted, by checking the required service directory check boxes.
3. Click **OK** in the warning message window to delete the selected directory services.

**Related Links**

[Editing a Directory Service](#)

## Importing Users

The **Import Active Directory Users** option allows you to import various active directory users into ASM. Perform the following tasks to import the users into ASM software:

📝 **NOTE:** Prior to importing Active Directory users, you must create at least one directory service through ASM. After importing the users, these users can log in to ASM virtual appliance using the following format: <ASM Directory Service Name>/ <user name>, and then type the password. If an imported user is deleted from Active Directory, that user is not automatically deleted from ASM. The deleted user cannot log in to the virtual appliance, and you must remove the user manually from the user list.

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

5. Select one or multiple users in the **Selected Users List** and click **Apply** to import the users.

> 📝 NOTE: While importing Active Directory users, ASM roles are not automatically mapped to Active Directory user roles. Therefore, it is important to assign an appropriate role level to each imported user.

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

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

## About Roles

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.

- **Administrator**: 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 ASM license

**Related Links**

> [Generating a Troubleshooting Bundle](#)
> [Editing Default Time Zone and NTP Settings](#)
> [Generating a Certificate Signing Request](#)
> [Downloading the Certificate Signing Request](#)
> [Uploading an SSL Certificate](#)
> [Editing Proxy Settings](#)
> [License Management](#)

## Generating a Troubleshooting Bundle

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

1. In the left pane, click **Settings**, and then click **Virtual Appliance Management**.
2. On the **Virtual Appliance Management** page, click **Generate Troubleshooting Bundle**.
3. Open or save the file.

## Generating and Uploading the SSL Certificates

Uploading an SSL certificate provides the following advantages:

- Ensures secure transmission by encrypting data that ASM sends over the web
- Provides authentication and ensures data is routed to its intended endpoint
- Prevents users from receiving browser security errors

To upload an SSL certificate:

1. Generate a Certificate Signing Request (CSR).
2. Download the CSR.
3. Submit the CSR to a Certificate Authority (CA). The CA provides a valid SSL certificate.
4. Upload the SSL certificate to ASM.

**Related Links**

> [Generating a Certificate Signing Request](#)
> [Downloading the Certificate Signing Request](#)
> [Uploading an SSL Certificate](#)

### Generating a Certificate Signing Request

A Certificate Signing Request (CSR) includes server information (such as domain name, locale) that certificate authorities require to provide a valid SSL certificate.

After generating the CSR, download the encrypted text, and then submit it to a certificate authority. The Certificate Authority provides a valid SSL certificate for you to upload.

1. In the left pane, click **Settings**, and then click **Virtual Appliance Management**.
2. On the **Virtual Appliance Management** page, under the **SSLCertificates** section, click **Generate Certificate Signing Request**.

   a. In the **Distinguished Name (www.domain.com)** box, type a distinguished name in the format www.domain.com.

   b. In the **Business Name** box, type a business name where the certificate is recorded.

   c. In the **Department Name** box, type a department name of the organizational unit (for example, IT, HR, or Sales) for which the certificate is generated.

   d. In the **Locality (Town/City)** box, type a locality name in which the organization is located.

   e. In the **State (Province/Region)** box, type a state name in which the organization is located (do not abbreviate).

   f. From the **Country** drop-down list, select a country in which the organization is located.

   g. In the **Email** box, type a valid email address.

   h. Click **Generate**.

3. Click **Download Certificate Signing Request**, and then copy the text that is displayed. To receive a valid SSL certificate, submit this text to a certificate authority.

### Downloading the Certificate Signing Request

After generating the CSR, download the resulting text and submit it to a certificate authority. The certificate authority provides an SSL certificate for you to upload to ASM.

1. In the left pane, click **Settings**, and then click **Virtual Appliance Management**.
2. On the In the **Virtual Appliance Management** page, under the **SSLCertificates** section, click **Download Certificate Signing Request**.
3. To receive a valid SSL certificate, copy the displayed text and then submit it to a certificate authority.

After the certificate authority provides the SSL certificate, upload it to ASM.

### Uploading an SSL Certificate

Before you upload an SSL certificate, generate and download a certificate signing request (CSR). To receive a valid SSL certificate, submit the CSR to a certificate authority. Save the certificate to a local network share.

1. In the left pane, click **Settings**, and then click **Virtual Appliance Management**.
2. On the **Virtual Appliance Management** page, under the **SSLCertificates** section, click **Upload Certificate**.
3. Click **Browse**, and select an SSL certificate.
4. To upload the certificate, click **Save**.
5. Confirm or cancel the action when a confirmation message is displayed.

After uploading the certificate, the GUI becomes unavailable as the web services are restarted, the virtual appliance shell is still accessible and all active users are logged out.

## Editing Proxy Settings

If your network uses a proxy server for external communication, then you must type the critical information to enable communication with ASM virtual appliance.

1. In the left pane, click **Settings**, and then click **Virtual Appliance Management**.
2. On the **Virtual Appliance Management**, under the **Proxy Settings** section, click **Edit**.
3. Select **Use HTTP Proxy Settings**.
4. In the **Server Address (IP or Hostname)** box, type a server address for the proxy server.
5. In the **Port** box, type a valid port number from 1–65535. Commonly used ports for a proxy server are 80 and 8080.
6. If the proxy server requires credentials to log in, select **Use Proxy Credentials** and then in **User Name** and **Password** boxes, type the required user name and password. To verify the password, type the password in **Confirm Password**.
7. To validate the settings typed on this page, click **Test Proxy Connection**.
8. Click **Save**.

## License Management

ASM licensing is based on the total number of managed resources.

The valid license type supported is Standard license. Standard license is a full-access license type. After uploading an initial license, you can upload subsequent licenses on the **Virtual Appliance Management** page. Subsequent uploads will replace the existing license.

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

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

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

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

## Editing Default Time Zone and NTP Settings

Changes on this page affect the time zone and NTP server(s) that are applied to ASM virtual appliance. All time data is stored in UTC format, and is used to display log and event time stamps.

1. In the left pane, click **Settings**, and then click **Virtual Appliance Management**.
2. On the **Virtual Appliance Management** page, under the **Time Zone and NTP Settings** section, click **Edit**.
3. From the **Time Zone** drop-down list, select a time zone.
4. Type the IP address or hostname in **Preferred NTP Server** and **Secondary NTP Server (optional)** for time synchronization.

5. Click **Save**. The GUI becomes unavailable as the web services are restarted, the virtual appliance shell is still accessible and all active users are logged out.

# Virtual Identity Pools

In ASM, virtual identity pools provide a conceptual way to categorize the virtual identities that help in network communication.

A virtual identity pool can include any combination of following virtual identities:

- MAC
- IQN
- WWPN
- WWNN

By default, virtual identities that are not assigned to any virtual identity pool are automatically assigned to the *Global* pool.

After creating a virtual identity pool, you can assign the virtual identity pool to one or more templates. For example, you might create a virtual identity pool to use for specific business units, such as Finance, Human Resource, and for any specific application.

The **Virtual Identity Pools** page displays the following information about the virtual identity pools that are configured in ASM:

- **Name** — Displays the name of the virtual identity pool.
- **Description** — Displays the description to identify the virtual identity pool.
- **Created By** — Displays the name of the user who created the virtual identity pool.
- **Created Date** — Displays the time that the virtual identity pool was created and last modified.

In the **Virtual Identity Pools** page, click an existing virtual identity pool to see the following information about the virtual identity pools in the **Summary** tab:

- **Selected Prefix** — Displays the prefix that will be added to the beginning of the virtual identities.
- **Reserved** — Displays the total number of virtual identities reserved for future use.
- **Assigned** — Displays the total number of virtual identities assigned to the resources.
- **Available** — Displays the total number of virtual identities available in the virtual identity pool.
- **Auto Generate** — Indicates whether auto generate virtual identity pools option is enabled or disabled.

To edit the virtual identity pools information, click **Update Pool Identities** at the bottom of the **Summary** tab.

On the **Virtual Identity Pools** page, you can:

- Create virtual identity pools
- Export virtual identity pools
- Delete virtual identity pools

**Related Links**

> Creating Virtual Identity Pools

## Creating Virtual Identity Pools

The **Create Virtual Identity Pool** wizard enables you to create virtual identity pools and add virtual identities to the virtual identity pools.

To create a virtual identity pool:

1. In the left pane, click **Settings**, and then click **Virtual Identity Pools**.
2. In the **Virtual Identity Pools** page, click **Create**.

   The **Create Virtual Identity Pool** wizard is displayed.
3. On the **Pool Information** page, type the **Pool Name** and **Pool Description** to identify the virtual identity pool, and then click **Next**.

   The virtual identity pool name must be less than 100 characters.
4. On the **Virtual MAC** page, add the virtual MAC identities, and then click **Next**.
5. On the **Virtual IQN** page, add the virtual IQN identities, and then click **Next**.
6. On the **Virtual WWPN** page, add the virtual WWPN identities, and then click **Next**.
7. On the **Virtual WWNN** page, add the virtual WWNN identities, and then click **Next**.
8. On the **Summary** page, click **Finish**.

**Related Links**

[Adding Virtual MAC Identities](#)
[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 and 1,024).
2. From the **MAC Address Prefix** list, type the MAC address prefix to be added to the beginning of the MAC addresses.
3. Select **Auto Generate Identities if needed during deployments** check box to automatically generate the Virtual MAC address during the deployment, if required.

### Adding Virtual IQN Identities

At a time, you can add as less as one and as many as 1,024 virtual IQN identities at one time. The maximum number of virtual IQN identities that ASM can manage is 16,000.

1. On the **Virtual IQN** page of the Create Virtual Identity Pool wizard, in the **Number of Virtual iSCSI Identities** box type the total number of virtual IQN identities that you want to add (any whole number between 1 and 1,024).
2. In the **IQN Prefix** box, type the IQN prefix that to be added at the beginning of the IQN.

   Examples of possible prefixes include product types, serial numbers, host identifiers, and software keys.

   > NOTE: The IQN prefix cannot exceed 213 characters, must contain only alphanumeric characters (uppercase and lowercase), and the following special characters: − _ , : .
3. Select **Auto Generate Identities if needed during deployments** check box to automatically generate the Virtual IQN addresses during the deployment, if required.

### Adding Virtual WWPN Identities

At a time, you can add as few as one and as many as 1,024 virtual WWPN identities. The maximum number of virtual WWPN identities that ASM can manage is 16,000.

1. On the **Virtual WWPN** page of the Create Virtual Identity Pool wizard, in the **Number of Virtual WWPN Identities** box, type the total number of virtual WWPN identities that you want to add (any whole number between 1 and 1,024).
2. From **WWPN Prefix** drop-down list, select the WWPN prefix to be added to the beginning of the WWPN.
3. Select **Auto Generate Identities if needed during deployments** check box to automatically generate the Virtual WWPN addresses during the deployment, if required.

### Adding Virtual WWNN Identities

At a time, you can add as few as one and as many as 1,024 virtual WWNN identities. The maximum number of virtual WWNN identities that ASM can manage is 16,000.

1. On the **Virtual WWNN** page of the Create Virtual Identity Pool wizard, in **Number of Virtual WWNN Identities** type the total number of virtual WWNN identities that you want to add (any whole number between 1 and 1,024).
2. From the **WWNN Prefix** drop-down list, select the WWNN prefix to be added to the beginning of the WWNN.
3. Select **Auto Generate Identities if needed during deployments** check box if you want to automatically generate the Virtual WWNN addresses during the deployment.

## Deleting Virtual Identity Pools

> NOTE: You cannot delete a *Global* virtual identity pool, and you cannot delete the virtual identity pools that are currently associated with a template or if the virtual identity pools contain identities in an `Assigned` or `Reserved` state.

1. In the left pane, click **Settings**, and then click **Virtual Identity Pools**.
2. On the **Virtual Identity Pools** page, select the check boxes next to the virtual identity pools that you want to delete, and then click **Delete**.

**3.** Click **OK** when the confirmation message is displayed.

**Related Links**

[Creating Virtual Identity Pools](#)

[Exporting Virtual Identity Pools](#)

## Exporting Virtual Identity Pools

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

**1.** In the left pane, click **Settings**, and then click **Virtual Identity Pools**.

**2.** On the **Virtual Identity Pools** page, select the virtual identity pools detail that you want to export, and then click **Export**.

**3.** Open or save the file.

**Related Links**

[Creating Virtual Identity Pools](#)

[Deleting Virtual Identity Pools](#)

# Troubleshooting

This chapter includes details for resolving common issues encountered in ASM 7.6.

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.

## ESXi and Hyper-V host deployments using network storage only support certain configurations

Currently, only CHAP authentication is supported while deploying ESXi. If you select an EqualLogic component with IP/IQN authentication, the service cannot be deployed. Currently, while deploying Hyper-V, exactly two EqualLogic storage volumes using IP/IQN authentication are required. For Hyper-V, CHAP authentication is not supported.

## iSCSI storage network only support static IP addressing

Currently, while creating a network in ASM for iSCSI connectivity, specify the network using static IPs. Setting an iSCSI network to DHCP causes issues during deployment.

## Unable to deploy a service for Compellent component with same server object and volume names

You cannot deploy a service for Compellent component if the server object is already mapped to the volume. This error occurs because a volume name available in recycle bin is same as the volume that the resource module is trying to create using ASM UI.

You must have unique names for Volumes and Server Objects in the system (even if the volumes and server objects are in different folders) because of the issues caused in Compellent API and UI behavior.

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

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

In ASM 7.6 release, you cannot create a template with two EqualLogic CHAP components and deploy a service that includes ESXi hosts attached to storage. Currently, ESXi deployments support a single EqualLogic component.

## Unable to log in to ASM using Active Directory using "\"

You cannot log in to ASM using Active Directory with the domain name and user name separated by back slash "\".

To log in to ASM using Active Directory, use forward slash "/". For example: <domain>/ <username>.

**NOTE:** Domain is the name for the Active Directory service you have created in ASM.

## Chain Booting issue occurs while booting microkernel in a multi-hop DHCP environment

The chain booting error occurs if the DHCP server is configured in a different subnet or network or connected to a different switch.

In such scenarios, the DHCP network is tagged.

To resolve this issue, in switch configuration, modify the native VLAN of server or computer facing ports to PXE VLAN.

Sample native VLAN configuration in Dell PowerConnect switch:

*interface Gi1/0/2*

*spanning-tree portfast*

*switchport mode general*

*switchport general pvid 3000*

*switchport general allowed*

*vlan add 3000*

*switchport general allowed*

*vlan add 20,30,40 tagged*

*exit*

In the above example:

- 3000: Indicates Native PXE VLAN
- 20,30,40: Indicates Management or vMotion or ISCSI

In case of production environments with large networks, routers may be configured with IP Helper Addresses to point to a DHCP on another network.