# Contents

Revision history ........................................................................................................................... 7

Introduction .................................................................................................................................. 8

AMP-VX overview ........................................................................................................................ 9
  AMP-VX layers ............................................................................................................................. 10
    Hardware layer .......................................................................................................................... 10
    Hypervisor layer ....................................................................................................................... 10
    Management workload layer ..................................................................................................... 11
    Application layer ..................................................................................................................... 11
  Architecture and components ...................................................................................................... 13
  Base configurations and scaling .................................................................................................. 13

Storage ......................................................................................................................................... 15

Network (VMware vSphere 6.7) .................................................................................................. 16
  Network architecture and design (VMware vSphere 6.7) .............................................................. 18
  Inter-VxBlock System connectivity use case (VMware vSphere 6.7) .............................................. 20
  Virtual networking (VMware vSphere 6.7) .................................................................................. 22
    VMware vSphere Distributed Switch design (VMware vSphere 6.7) ......................................... 23
    VM placement and VLAN assignment (VMware vSphere 6.7) .................................................. 24

Virtualization (VMware vSphere 6.7) .......................................................................................... 26
  VMware vSphere ESXi (VMware vSphere 6.x) ........................................................................... 26
  VMware vCenter Server (VMware vSphere 6.x) ......................................................................... 26
    VxBlock System VMware vCenter Server (VMware vSphere 6.x) ............................................. 27
    AMP-VX VMware vCenter Server (VMware vSphere 6.7) .......................................................... 27
  Management workloads (VMware vSphere 6.x) ......................................................................... 28

Manage the AMP (VMware vSphere 6.7) .................................................................................... 30
  Management software components (VMware vSphere 6.x) ....................................................... 30
  Configure system monitoring (VMware vSphere 6.x) ................................................................. 31
  Manage VMware vSphere operations (VMware vSphere 6.7) .................................................... 32
    Monitor VMware vSAN (VMware vSphere 6.7) ..................................................................... 32
    Prepare the VMware vSphere ESXi server for temporary maintenance (VMware vSphere 6.7) . 32
    Prepare the VMware vSphere ESXi server for shutdown (VMware vSphere 6.7) .................... 33
    Boot the VMware vSphere ESXi host (VMware vSphere 6.7) .................................................. 33
    Install the latest VMware vSphere ESXi patch (VMware vSphere 6.7) .................................... 34
    Patch VMware vSphere ESXi hosts with the VMware vSphere Update Manager (VMware vSphere 6.7) .......................................................... 35

Manage VMware Single Sign On (VMware vSphere 6.x) ............................................................. 37
  Unlock and reset the VMware Single Sign On administrator password (VMware vSphere 6.x) . 37
  Manage the lockout status of VMware Single Sign On (VMware vSphere 6.x) ......................... 38
  Manage VMware Single Sign On default password policies (VMware vSphere 6.x) ................. 38
  Manage VMware Single Sign On lockout policies (VMware vSphere 6.x) ............................... 38
  Add an AD identity source to VMware Single Sign On (VMware vSphere 6.7) ........................... 39
  Install VMware vCenter Server root certificates on a web browser (VMware vSphere 6.x) ......... 40
  Redirect VMware vCenter Server to the secondary external VMware Platform Services Controller (VMware vSphere 6.x) .......................................................... 40

Network (VMware vSphere 6.5) .................................................................................................. 41
  Network architecture and design (VMware vSphere 6.5) ............................................................ 44
Contents

Inter-VxBlock System connectivity use case (VMware vSphere 6.5) ................................................................. 50
Virtual networking (VMware vSphere 6.5) ........................................................................................................... 52
   VMware vSphere Standard Switch design (VMware vSphere 6.5) ................................................................. 53
   VMware vSphere Distributed Switch design (VMware vSphere 6.5) ............................................................. 54
   VM placement and VLAN assignment (VMware vSphere 6.5) ....................................................................... 56

Virtualization (VMware vSphere 6.5) .................................................................................................................. 61
   VMware vSphere ESXi (VMware vSphere 6.x) ................................................................................................. 61
   VMware vCenter Server (VMware vSphere 6.5) ............................................................................................. 61
   VxBlock System VMware vCenter Server (VMware vSphere 6.x) ................................................................. 62
   AMP-VX VMware vCenter Server (VMware vSphere 6.5) .............................................................................. 62
   Management workloads (VMware vSphere 6.x) .............................................................................................. 63

Manage AMP-VX (VMware vSphere 6.5) ........................................................................................................... 65
   Management software components (VMware vSphere 6.5) ......................................................................... 65
   Configure system monitoring (VMware vSphere 6.x) ...................................................................................... 66
   Manage VMware vSphere operations (VMware vSphere 6.5) ....................................................................... 67
      Monitor VMware vSAN (VMware vSphere 6.5) .......................................................................................... 67
      Prepare the VMware vSphere ESXi server for temporary maintenance (VMware vSphere 6.5) .............. 67
      Prepare the VMware vSphere ESXi server for shutdown (VMware vSphere 6.5) .................................... 68
      Boot the VMware vSphere ESXi host (VMware vSphere 6.5) ................................................................. 68
      Install the latest VMware vSphere ESXi patch (VMware vSphere 6.5) .................................................... 69
      Patch VMware vSphere ESXi hosts with the VMware vSphere Update Manager (VMware vSphere 6.5) .... 70
   Manage VMware Single Sign On (VMware vSphere 6.x) ............................................................................ 72
      Unlock and reset the VMware Single Sign On administrator password (VMware vSphere 6.x) ............... 72
      Manage the lockout status of VMware vCenter SSO (VMware vSphere 6.7) ........................................... 72
      Manage the lockout status of VMware Single Sign On (VMware vSphere 6.5) ....................................... 73
      Manage VMware vCenter SSO default password policies (VMware vSphere 6.7) ................................. 73
      Manage VMware Single Sign On default password policies (VMware vSphere 6.0 or 6.5) .................... 73
      Add Windows AD identity source to VMware SSO (VMware vSphere 6.7) ............................................. 74
      Add a Windows AD identity source to VMware vCenter SSO (VMware vSphere 6.5) ......................... 75
      Install VMware vCenter Server root certificates on a web browser (VMware vSphere 6.x) ............... 76
      Redirect VMware vCenter Server to the secondary external VMware Platform Services Controller (VMware vSphere 6.x) .............................................................................................................. 76

Manage multiple VxBlock Systems .................................................................................................................. 77

AMP-VX Integrated Data Protection ................................................................................................................ 79
   Avamar Virtual Edition and Data Domain ....................................................................................................... 80
   Avamar Virtual Edition and VMware vCenter Server Appliance ................................................................ 81
   Avamar checkpoints ...................................................................................................................................... 81
   Application-specific scripted backups .......................................................................................................... 81
   Password security .......................................................................................................................................... 82
   Update the CPSD-DP-Settings.cfg file .......................................................................................................... 83
   Perform VMware PSC backups in a VMware ELM environment ................................................................... 85
   Create the scheduled tasks for all backups ................................................................................................... 89
   Backup types and locations for Avamar and scripted backups ................................................................... 89
   Restore from backup ....................................................................................................................................... 91
      Restore an Avamar image using the Avamar Administrator Console ...................................................... 91
      Restore an Avamar image using VMware vSphere Web Client ............................................................... 92
      Restore an instant access Avamar image using the VMware vSphere Web Client .................................. 92
      Restore files from a file-level backup using the Avamar Administrator console ................................... 93
      Restore files from an image backup using the Avamar Administrator console ..................................... 93
      Restore AMP-VX management VMs ........................................................................................................ 94
      Restore the element manager for storage arrays VM from an Avamar image backup ......................... 94
      Restore the element manager for the data protection VM ..................................................................... 94
# Revision history

<table>
<thead>
<tr>
<th>Date</th>
<th>Document revision</th>
<th>Description of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 2019</td>
<td>1.8</td>
<td>Added information about support for external versus embedded PSCs. Added note to <em>Application layer</em> that as of RCM 6.5.10.0 and 6.7.3.0, Cisco DCNM is not supported.</td>
</tr>
<tr>
<td>April 2019</td>
<td>1.7</td>
<td>Added support for Integrated Data Protection script updates.</td>
</tr>
<tr>
<td>March 2019</td>
<td>1.6</td>
<td>Added support for VxBlock Central, VMware VDS, and VMware vSphere 6.7.</td>
</tr>
<tr>
<td>December 2018</td>
<td>1.5</td>
<td>Updated Overview section.</td>
</tr>
<tr>
<td>October 2018</td>
<td>1.4</td>
<td>Added support for VMware NSX 6.4 for VxBlock System 1000.</td>
</tr>
<tr>
<td>August 2018</td>
<td>1.3</td>
<td>Added support for Cisco Nexus 9336C-FX2 switch as a management switch.</td>
</tr>
<tr>
<td>March 2018</td>
<td>1.2</td>
<td>Added information about changing passwords.</td>
</tr>
<tr>
<td>March 2018</td>
<td>1.1</td>
<td>Added data protection backup procedures and administrative tasks.</td>
</tr>
<tr>
<td>February 2018</td>
<td>1.0</td>
<td>Initial version</td>
</tr>
</tbody>
</table>
Introduction

This guide describes the high-level design, including hardware and software components of the Dell EMC AMP-VX management solution and instructions for managing AMP-VX after installation.

This guide describes all the features and components that are supported on AMP-VX. Some features or components that are documented in this guide may not be required to manage your VxBlock System.

The target audience for this guide includes those responsible for managing AMP-VX, sales engineers, field consultants, and advanced services specialists.

For these tasks, this guide assumes that the person has troubleshooting skills and is familiar with:

- VMware vSAN technologies
- AMP-VX concepts and terminology

The Glossary provides terms, definitions, and acronyms related to VxBlock Systems.
AMP-VX overview

Manage multiple VxBlock Systems 1000 from a single, shared management platform using AMP-VX.

Besides virtualization and compute components, AMP-VX contains a core set of management workloads to manage VxBlock 1000. Management tools are installed and configured on the AMP-VX. AMP-VX uses components and workloads to provide local management and management software to install and operate VxBlock 1000 components.

AMP-VX can rapidly adapt and respond to growing and changing management capabilities that Dell EMC supports. With AMP-VX, you can:

- Run core and Dell EMC optional management workloads.
- Monitor health and manage performance and capacity.
- Provide network and fault isolation.

A VxBlock 1000 with an AMP-VX can centrally manage the following attached systems:

- VxBlock System 340
- VxBlock System 350
- VxBlock System 540
- VxBlock System 740

Central management of these platforms is an in-field consolidation service of AMP-2S managed Converged Systems. Central management requires assessment and sizing to verify that the additional AMP-2S workloads can be consolidated onto the AMP-VX. Core management VMs are migrated from the AMP-2S on each VxBlock System and consolidated onto the AMP-VX.

Contact your Dell EMC representative for more information on central management.

VxBlock Central

VxBlock Central is available in a Base option, Workflow Automation option, and Advanced Analytics option.

Up to eight VxBlock System can be managed by AMP-VX. The AMP-VX contains a single instance of VxBlock Central, VxBlock Central Orchestration Services, and VMware vRealize Orchestrator regardless of the number of VxBlock Systems consumed (within maximum allowed) by VxBlock Central Orchestration.

See the Dell EMC VxBlock System 1000 Architecture Overview for more information about VxBlock Central.

Support

The following systems support AMP-VX centralized management:

- VxBlock Systems managed by a VxBlock 1000 with AMP-VX and an in-field consolidation service. Other AMP models are not supported for consolidation.
- Only VxBlock Systems managed by AMP-2S are eligible for in-field consolidation service. Other AMP models are not supported for consolidation.
- VxBlock Systems managed by VxBlock 1000 with AMP-VX running NSX are not eligible for in-field consolidation service.
- VxBlock Systems managed by VxBlock 1000 with AMP-VX with an HBA requirement are not eligible for in-field consolidation service.
- VxBlock Systems that require an FC-HBA for VMAX storage management or have other SAN FC-HBA dependencies are not supported by AMP-VX:
  - Use cases, such as EHC, require an FC-HBA connection to the VMAX ViPR Controller. ViPR supports only an FC connection to the VMAX.
Systems that require an FC-HBA connection to the VMAX can maintain that connection and software that uses it with the existing legacy AMP.

**AMP-VX layers**

AMP-VX is comprised of an application layer, a management workload layer, a hypervisor layer and a hardware layer. The following illustration shows the components in each layer of AMP-VX:

**Hardware layer**

AMP-VX uses Dell PowerEdge Server technology in the hardware layer. Internal disk drives and VMware vSAN provide shared storage for the AMP-VX management platform. The VxBlock System provides the following for AMP-VX:

- Network components that are used by AMP-VX for management and data planes.
- Network switching to connect to the management platform for AMP-VX to manage the VxBlock System.

AMP-VX also comes with Integrated Data Protection and includes a Data Domain backup appliance.

**Hypervisor layer**

VMware vSphere Enterprise Plus is the default hypervisor on the AMP-VX host. VMware vSphere Enterprise Plus requires less than 6 GB of storage to install and has minimal management overhead. VMware vSphere Enterprise Plus provides the following features:

- VMware High Availability (HA)
• VMware Layer 3 vMotion capability
• VMware Fault Tolerance
• VMware Dynamic Resource Scheduling (DRS)
• VMware CPU and memory resource pools (for VMware standard switches)

On the AMP-VX, the VMware vSphere Hypervisor ESXi boots from Dell Server Secure Digital High Capacity/Secure Digital eXtended Capacity (micro SDHC/SDXC) cards. VMware vSphere ESXi does not contain a console operating system.

VMware vSphere Hypervisor ESXi on production Cisco servers boots from internal SD cards (default) or from SAN.

Management workload layer

The management workload layer classifies the workload type of the management applications.

The management workload applications are required components of:
• AMP-VX and VxBlock System (core)
• An optional and supported component (Dell EMC optional), or
• An ecosystem component not engineered as part of the VxBlock System (ecosystem).

The following table describes the management workloads:

<table>
<thead>
<tr>
<th>Management workload</th>
<th>Description</th>
</tr>
</thead>
</table>
| Core                 | Minimum set of required management software that is engineered and supported on the AMP-VX and VxBlock System including:  
|                      | • All hypervisor management
|                      | • Element Managers
|                      | • Virtual networking components
|                      | • Vision Intelligent Operations or VxBlock Central
|                      | • AMP-VX Integrated Data Protection |
| Dell EMC optional    | Non-core management workloads that are covered by Dell EMC support and installed by Dell EMC. These applications are optional components on the VxBlock System and are not required to manage the VxBlock System. |
| Ecosystem            | These applications have not been engineered as part of the VxBlock System, but can be installed on it subject to the specific sizing guidelines of the application itself. Ecosystem workloads always require more servers be added to the AMP-VX to support that workload.  
|                      | Ecosystem management applications are limited to Dell EMC System Ready Certified, or Cisco, Dell EMC, or VMware applications (for example, Cisco Intelligent Automation for Cloud and Cloud Orchestration). |

Application layer

The application layer contains the core management, optional management, and ecosystem management workloads for AMP-VX.

The following table describes key software components for AMP-VX management workloads:
## Workloads Components

### Core management
- Hypervisor management
  - VMware vCenter Server for AMP-VX
  - VMware vCenter Server
- Element Managers
- VMware vRealize Log Insight
- VxBlock Central
- Secure Remote Services
- Avamar Virtual Edition
  - Licensed version for AMP-VX Integrated Data Protection
  - Evaluation version for VxBlock System data backup
- Avamar Administrator
- Data Domain Virtual Edition (evaluation for data backup)

More core management software components that may be added depending on the VxBlock System requirements. The list includes, but is not limited to the following:
- Cisco Data Center Network Manager (DCNM)
  - Note: As of RCM 6.5.10.0 and 6.7.3.0, Cisco DCNM is no longer supported.
- PowerPath License Manager
- VMware vSphere NSX Manager

### Dell EMC optional management
This list includes, but is not limited to the following:
- Integrated Data Protection, security, or storage management tools
- Unisphere for VMAX
- Unisphere 360
- Unisphere Central
- RecoverPoint or VPLEX
- Solutions Enabler with SMI-S Provider
- VMware vCloud Network and Security appliances (vShield Edge/Manager)
- VMware vRealize Operations Manager
- VMware vCenter Site Recovery Manager
- Data Protection Central
- VxBlock Central Orchestration
- VxBlock Central Orchestration Services
## Workloads and Components

This list includes, but is not limited to the following:

- VMware vCloud Director
- Cisco Intelligent Automation for Cloud
- Cisco UCS director
- ViPR Controller
- Cisco UCS central

## Architecture and Components

The VxBlock System provides network resources to AMP-VX which contains compute, storage, virtualization, and management resources.

AMP-VX is available in a fixed server configuration that uses its own resources to run workloads without consuming resources on the VxBlock System. AMP-VX contains 4-64 Dell PowerEdge R640 servers, each of which include the following components:

- One rack unit single-socket R640 server
- 384-Gb Memory
- 20 core, 2.4-GHz CPU
- SD card for VMware vSphere ESXi boot
- VMware vSAN all flash shared storage
- 14-TB raw usable storage per server
- Trusted Platform Module (TPM) 1.2 enabled (optional)

This fixed configuration is available for VxBlock System management workloads. AMP-VX servers are single-socket, one rack unit, rack mount server built for production-level applications.

AMP-VX can be deployed in numerous system sizes, however the minimum is four servers. Add AMP-VX servers in increments of one, as required, up to 64 nodes in a single VMware vSAN cluster.

The base AMP-VX configuration of four servers supports the core management workload for the AMP-VX and one VxBlock System plus any optional workloads that are not related to data protection. Servers can be added to manage multiple VxBlock Systems or to increase workload capacity for data protection and ecosystem applications.

VMware vSAN cluster can scale to 64 servers. The true scale of the AMP-VX platform depends on the number of physical network ports available on the VxBlock System.

## Base configurations and scaling

AMP-VX has a base configuration with a minimum set of fixed compute components.

AMP-VX is integrated within one or more standard cabinets of the VxBlock System or deployed within a stand-alone cabinet. Within the base configuration, the following hardware is included:

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Minimum set</th>
</tr>
</thead>
<tbody>
<tr>
<td>PowerEdge R640</td>
<td>4 servers to support performance and resiliency features of VMware vSAN.</td>
</tr>
<tr>
<td>Network</td>
<td>1 x quad port 10 GbE Base-T</td>
</tr>
<tr>
<td></td>
<td>2 x dual port 10/25-GbE SFP+ NIC</td>
</tr>
</tbody>
</table>
The system requirements for the default AMP-VX software applications and core software components of a VxBlock System determine the base configuration of AMP-VX.

The following AMP-VX base software is used to determine the minimum configuration of AMP-VX:

- Vision Intelligent Operations or VxBlock Central
- VMware vSphere and one instance VMware vCenter Server Appliance (vCSA) for AMP-VX
- Secure Remote Services (two gateways)
- Windows Server (2 VMs)
- Avamar Virtual Edition (2 TB)
- VMware vRealize Log Insight (three-node cluster)
- Avamar Virtual Edition (.5 TB) trial edition
- Data Domain Virtual Edition (.5 TB) trial edition

The following VxBlock System software is used to determine the minimum configuration of AMP-VX:

- Two instances of VMware vCSA
- PowerPath License Manager
- Cisco DCNM LAN and SAN (large)
- XtremIO Management Server (expanded)
- Isilon InsightIQ
- Unisphere for VMAX (medium)
- Unisphere 360 for VMAX
- Unisphere Central (medium)
- VMware vRealize Operations Manager
- VMware NSX Manager

AMP-VX is a scale-out solution that enables you to add AMP-VX servers, as needed, to meet the system resource requirements for planned management workloads. VMware vSAN software-defined storage enables scaling from a base configuration to a large-scale deployment up to 64 servers in a single VMware vSAN cluster. Although the VMware vSAN cluster can scale to 64 servers, the true scale of the AMP-VX platform depends on the number of physical network ports available on VxBlock Systems.

These resources can be scaled up as necessary to meet increasingly stringent application workload requirements. To scale up AMP-VX resources, add servers to the environment.

Verify that all planned workloads run successfully on N-2 servers to enable the environment to withstand a two-server outage without impact. The addition of data protection software for external data or a third VxBlock System VMware vCSA requires at least one more AMP-VX server. Understanding sizing of the planned workloads is critical to building an appropriate AMP-VX solution.
AMP-VX uses VMware vSAN software-defined storage technology with all flash storage.

VMware vSAN is an enterprise, software-only storage solution that uses the local drives and network ports of existing AMP-VX system servers. With these drives and ports, AMP-VX creates a single, high performance, shared datastore that all hosts in the AMP-VX VMware vCenter Server cluster can use. It is designed to scale to 64 servers per VMware vSAN cluster.

For more information about VMware vSAN, refer to the VMware website.

Related information
VMware.com
Network (VMware vSphere 6.7)

VxBlock Systems 1000 offer several types of management network connectivity and server assignments. The AMP-VX connects to the management and data switches in the VxBlock System 1000.

AMP-VX servers connect to the VxBlock 1000 ToR switches with 1 x dual port 10/25-GbE SFP+ NICs (one port per switch) to communicate with in-band components of the infrastructure. Depending on the capability of the switch, the connection is either a 25-GbE SFP+ direct connect cable or a 10-GbE SFP+ using breakout cables.

AMP-VX connects to the VxBlock 1000 management network switches using:

- 2 x 10-GbE Base-T ports for VMware vSAN, management data, and OOB components
- One 10-GbE Base-T port for the iDRAC connection for remote management of each AMP-VX server

Two ports connect to one switch (iDRAC and one port for VMware vSAN and OOB management). One port connects to the other switch (VMware vSAN and OOB management).

The following diagram shows VMware vSphere ESXi network connectivity on AMP-VX servers:
See the appropriate Architecture Overview to understand the specific network switch capabilities of the VxBlock System 1000 managed by AMP-VX.
Network architecture and design (VMware vSphere 6.7)

In a standard VxBlock System, most network connectivity between components is internal. Management network connectivity is accessible to any VxBlock System that the AMP-VX manages.

Layer 2 or 3 routing (default) is configured between the management plane and the external network to enable management functionality. These routing configurations are implemented at the management or management aggregation switches.

For L2 traffic, AMP-VX VLANs remain local to the management plane of the VxBlock Systems. AMP-VX uses VMware vSphere Distributed Switch (VDS).

The logical network design for AMP-VX reduces impact from network outages. The design optimizes the environment for advanced security implementations, such as Dell EMC secure administrative access and trusted multitenancy solutions. The VLAN design is similar to a standard VxBlock System.

AMP-VX uses the following types of networking:

- In-band management
- Out-of-band management
- Virtual

**In-band management networking**

The in-band management networking of the VxBlock System traverses the VxBlock System ToR network switches.

The following table shows VLANs that carry management traffic local to the managed VxBlock System and AMP-VX:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcesys_esx_mgmt</td>
<td>VxBlock System VMware management and applications that may impact production.</td>
</tr>
<tr>
<td>vcesys_esx_vmotion</td>
<td>VMware vSphere vMotion L3 traffic between VxBlock System VMware vSphere ESXi hosts.</td>
</tr>
<tr>
<td>vcesys_esx_ft</td>
<td>VMware fault tolerance traffic between VxBlock System VMware vSphere ESXi hosts.</td>
</tr>
<tr>
<td>vcesys_brs_data</td>
<td>Backup and recovery with data protection solution.</td>
</tr>
<tr>
<td>vcesys_nfs</td>
<td>NAS VLAN.</td>
</tr>
<tr>
<td>vcesys_esx_build</td>
<td>VLAN required for VM deployment.</td>
</tr>
</tbody>
</table>

The vcesys_nfs VLANs remain local (and internal) to each managed VxBlock System and are not routed through the core network.

The in-band management network of the AMP-VX traverses the VxBlock System management network switches. The AMP-VX in-band management network does not impact production use of the VxBlock System.

VMware vSphere ESXi VLANs that carry management traffic local to AMP-VX cannot be used for any production data.

The following table shows the VMware vSphere ESXi VLANs that carry management traffic local to AMP-VX:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>amx_esx_mgmt</td>
<td>AMP-VX VMware management and applications.</td>
</tr>
<tr>
<td>amx_esx_vmotion</td>
<td>VMware vSphere vMotion L3 traffic between AMP-VX VMware vSphere ESXi hosts.</td>
</tr>
<tr>
<td>amx_esx_ft</td>
<td>VMware fault tolerance traffic between AMP-VX VMware vSphere ESXi hosts.</td>
</tr>
<tr>
<td>amx_vCenter_ha</td>
<td>Optional VLAN for vCenter HA traffic</td>
</tr>
<tr>
<td>amx_brs_data</td>
<td>AMP-VX backup and recovery with Integrated Data Protection solution.</td>
</tr>
</tbody>
</table>
The `amx_esx_ft` VLANs remain local (and internal) to the AMP-VX and are not routed through the core network.

**Out-of-band management networking**

OOB networks do not impact production use of the VxBlock System. This traffic traverses the VxBlock System management switches.

Production data must not use any of the networks that are listed in the following table:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcesys_ipmi</td>
<td>Used for Data Domain IPMI. There is not data on this VLAN.</td>
</tr>
<tr>
<td>vcesys_oob_mgmt</td>
<td>VMs and device ports are used for control plane only. There is no data on this VLAN. Both the VxBlock System and the AMP-VX use this VLAN.</td>
</tr>
<tr>
<td>amx_vsan</td>
<td>AMP-VX VMware vSAN cluster network communications use this VLAN.</td>
</tr>
</tbody>
</table>

The `amx_vsan` VLAN remains local (and internal) to the AMP-VX and is not routed through the core network.

**Virtual networking**

The following table describes production and management VLANs:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Description</th>
</tr>
</thead>
</table>
| vcesys_esx_mgmt  | Carries inter-VxBlock System management traffic to and from the VMs in the XMP_Prod_Central management workload folder. The following specifications should be considered for this VLAN:  
- For L2 network connectivity, use a /22 subnet or larger to accommodate 650 to 2000 VMware ESXi hosts.  
- If L3 network connectivity is required, size the assigned subnet according to the number of VMs supporting the managed VxBlock System. Plan the subnet size to include three VMs per VMware vCenter instance.  
- L2 or L3 connectivity through the customer-provided network is required to establish management functionality between the AMP-VX and managed VxBlock System. |
| vcesys_oob_mgmt  | Carries inter-VxBlock System management traffic to and from the VMs in the XMP_Prod_Cmn_rp management workload folder. The following specifications should be considered for this VLAN:  
- For L2 network connectivity, use a /22 subnet or larger to accommodate 650 to 2000 VMware ESXi hosts.  
- If L3 network connectivity is required, ensure to size the subnet to accommodate all management VMs, KVMs, and system components requiring out of band management.  
- L2 or L3 connectivity through the customer-provided network is required to establish management functionality between the AMP-VX and managed VxBlock System. |

The following illustration shows an example of VLAN requirements and usage with VMware VDS:
Inter-VxBlock System connectivity use case (VMware vSphere 6.7)

The AMP-VX network architecture allows for a Layer 3 scenario to establish inter-VxBlock System connectivity. The host AMP-VX system must be in the same data center or within a metro 10 ms R/T latency distance of the VxBlock System it is managing.

The following table provides a L3 use case, requirements, and caveats:

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L3</td>
<td>Inter-VxBlock System connectivity using L3 capability.</td>
</tr>
<tr>
<td>Description</td>
<td>This option uses L3 routing between the AMP-VX VLANs and the VxBlock System VLANs for management traffic.</td>
</tr>
</tbody>
</table>
Use Case | Description
--- | ---
Requirements | The following management networks residing on the VxBlock System as well as the AMP-VX management VLANs must have L3 routing configuration implemented.
- vcesys_esx_mgmt
- vcesys_oob_mgmt
- amx_esx_mgmt

This enables management functionality between the AMP-VX and the managed VxBlock Systems. vcesys_oob_mgmt requires L3 routing to access applications running on management VMs that reside on the out-of-band network. vcesys_esx_vmotion (vMotion Netstack) and vcesys nfs remain local (and internal) to each of the managed VxBlock Systems and are not routed through the core network.

The following illustration shows VLANs configured on AMP-VX managing a VxBlock System and provides sample L3 routing configurations required on the core network layer (using VMware VDS):
Virtual networking (VMware vSphere 6.7)

AMP-VX includes virtual networking standards that allow each VM to connect to the physical network. Deploy the virtual networking components on the AMP-VX and place them in a manner to support a maximum level of redundancy (where choices are available).
VMware vSphere Distributed Switch design (VMware vSphere 6.7)

The AMP-VX VMware ESXi host has VMKernel, VM port groups, FT, and vMotion port groups configured on the ToR VMware vSphere Distributed Switch (VDS).

VMware vSAN, OOB, and Data Protection port groups are configured on the Management VMware VDS. Both of AMP-VX VMware VDS use NIOC to prioritize network traffic from VMs.

The following table shows the NIOC settings for the DVSwitch-MGMT distributed switches:

<table>
<thead>
<tr>
<th>Traffic type</th>
<th>Shares</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vSAN</td>
<td>High</td>
</tr>
<tr>
<td>NFS</td>
<td>Low</td>
</tr>
<tr>
<td>vMotion</td>
<td>Low</td>
</tr>
<tr>
<td>VMware vSphere replication</td>
<td>Low</td>
</tr>
<tr>
<td>Management</td>
<td>Normal</td>
</tr>
<tr>
<td>VMware vSphere Data Protection backup</td>
<td>Low</td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>High</td>
</tr>
<tr>
<td>Fault Tolerance</td>
<td>Low</td>
</tr>
<tr>
<td>iSCSI</td>
<td>Low</td>
</tr>
</tbody>
</table>

The following table shows the NIOC settings for the DVSwitch-ToR distributed switches:

<table>
<thead>
<tr>
<th>Traffic type</th>
<th>Shares</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSAN</td>
<td>Low</td>
</tr>
<tr>
<td>NFS</td>
<td>Low</td>
</tr>
<tr>
<td>VMware vMotion</td>
<td>Low</td>
</tr>
<tr>
<td>VMware vSphere replication</td>
<td>Low</td>
</tr>
<tr>
<td>Management</td>
<td>Normal</td>
</tr>
<tr>
<td>VMware vSphere Data Protection backup</td>
<td>Low</td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>High</td>
</tr>
<tr>
<td>Fault Tolerance</td>
<td>Low</td>
</tr>
<tr>
<td>iSCSI</td>
<td>Low</td>
</tr>
</tbody>
</table>

From the AMP-VX management folder, the AMP-VX VMware vCenter Server manages the AMP-VX ESXi host.

When hosting VMware vCenter Server environments for existing VxBlock Systems with Dell EMC legacy AMPs on the AMP-VX, consider the following:

- AMP-VX and existing VxBlock System compute hosts must be in the same datacenter and adhere to the 10 ms RTT latency limitations of AMP-VX.
- Any VxBlock System managed by AMP-VX must be at a supported RCM.
- VMware ESXi hosts from a VxBlock System cannot be included in the AMP-VX management vCenter.

To host existing VMware vCenter services, a dedicated VMware vCenter Server cluster with VMware DRS is created specifically for the existing VxBlock System under the production management folder. The VMs connect to the appropriate VM distributed port group within the VMware VDS.

The following illustration shows how the VMware VDS is configured on the AMP-VX:
VM placement and VLAN assignment (VMware vSphere 6.7)

The default VMware vCenter Server configuration contains the VMware vCenter Server 6.7 with Embedded Platform Services Controller.

Microsoft SQL is not used because VMware vCenter Server and VMware VUM use the bundled postgres database embedded within the VMware vCenter Server.

The following illustration provides an example of the VM server assignment for AMP-VX servers with the default configuration for VxBlock Systems:
Note: Actual placement of the management VMs is determined by high availability, VMware DRS, and affinity rules.

See the appropriate Architecture Overview for a description of specific management components of the Converged System managed by AMP-VX.
Virtualization (VMware vSphere 6.7)

VMware vSphere is the virtualization platform that provides the foundation for the private cloud. The core VMware vSphere components are the VMware vSphere ESXi and VMware vCenter Server for management. VMware vSphere 6.7 default deployment includes VMware vCenter Server with Embedded VMware Platform Services Controller (PSC) to provide the VMware Single Sign On (SSO) service.

Note: VMware vSphere 6.7 and VMware vSphere 6.5 are the last VMware vSphere releases that support the deployment of external PSCs. Updates to both of these VMware vSphere versions support Enhanced Linked Mode in embedded PSCs, making external PSCs no longer necessary. Upgrading to VMware vSphere 6.7 update 1 or VMware vSphere 6.5 update 2d enables you to migrate external PSCs to embedded PSCs. For more information about changing to embedded PSCs from external PSCs, consult with your account team.

The hypervisors are deployed in a cluster configuration. The cluster enables dynamic allocation of resources, such as CPU, memory, and storage. The cluster also provides workload mobility and flexibility with the use of VMware vSphere vMotion and Storage VMware vSphere vMotion technology.

VMware vSphere ESXi (VMware vSphere 6.x)

VMware vSphere ESXi Enterprise Plus is the system hypervisor.

Cluster configuration

VMware vSphere ESXi hosts and their resources are pooled together into clusters. These clusters contain the CPU, memory, network, and storage resources available for allocation to VMs. VMware vSphere clusters can scale up to a maximum of 64 hosts. Up to 2,000 hosts can be supported in one VMware vCenter Server instance.

Datastores

AMP-VX uses VMware vSAN for its storage which uses VSANFS as the on-disk format. The maximum size per volume is 62 TB. The maximum VMDK file size is 62 TB.

VMware vCenter Server (VMware vSphere 6.x)

The VMware vCenter Server provides a central management point for hypervisors and VMs.

VMware vCenter Server Appliance (vCSA) manages the virtual infrastructure. VMware vSphere Update Manager (VUM) is integrated with the VMware vCSA and assists with host patch management.

VMware vCenter Server with embedded PSC is the default deployment configuration offered.

Note: VMware vSphere 6.7 and VMware vSphere 6.5 are the last VMware vSphere releases that support the deployment of external PSCs. Updates to both of these VMware vSphere versions support Enhanced Linked Mode in embedded PSCs, making external PSCs no longer necessary. Upgrading to VMware vSphere 6.7 update 1 or VMware vSphere 6.5 update 2d enables you to migrate external PSCs to embedded PSCs. For more information about changing to embedded PSCs from external PSCs, consult with your account team.

There are at least two VMware vCSAs in the AMP: one for the AMP local management and one or more for the management of Converged Systems.

VMware vCSA provides the following functionality:

- Cloning of VMs
- Creating of templates
- Migration of VMs though VMware vSphere vMotion and VMware Storage vMotion
• Initial configuration of VMware Distributed Resource Services (DRS) and VMware vSphere high availability (HA) clusters

VMware vCSA monitor hosts and VMs and sends alerts. System administrators can create and apply alarms to all managed objects, including:
• Datacenter, cluster, and host health, inventory, and performance
• Datastore health and capacity
• VM usage, performance, and health
• Virtual network usage and health

Note: VMware vSphere 6.7 deployments disable the Host TPM attestation alarm definition at the factory to suppress attestation errors on installed but unused TPM modules.

Authentication
VMware Single Sign On (SSO) service integrates multiple identity sources including AD, open LDAP, and local accounts for authentication.

VMware vCenter Server supported features
Dell EMC supports the following VMware vCenter Server features:
• VMware Single Sign On (SSO) Service
• VMware vSphere Web Client (HTML5) for VMware vSphere 6.7 or VMware vSphere Web Client (used with VxBlock Central)
• VMware vSphere High Availability
• VMware Distributed Resource Scheduler (DRS)
• VMware vSphere Distributed Switch (vDS)
• VMware Fault Tolerance
• VMware vSphere vMotion
• VMware Storage vMotion
• VMware Enhanced vMotion Compatibility (EVC)
• VMware Storage Distributed Resource Scheduler (DRS) (capacity only)
• VMware Storage-driven profiles (user-defined only)
• VMware distributed power management (up to 50 percent of VMware vSphere ESXi hosts)
• VMware Syslog Service
• VMware Core Dump Collector

VxBlock System VMware vCenter Server (VMware vSphere 6.x)
The VxBlock System VMware vCenter Server manages the VMware vSphere ESXi environment of the VxBlock System.
The VxBlock System VMware vCenter Server uses VMware vSphere Distributed Switch (VDS) for virtual networking.

AMP-VX VMware vCenter Server (VMware vSphere 6.7)
The local management workload manages the AMP-VX VMware vSphere ESXi environment.
The AMP-VX VMware vCenter Server includes the following components:
• Virtual Network Switch: The AMP-VX VMware vCenter Server uses VMware vSphere Distributed Switches.
• Datacenter: The default AMP-VX configuration comes with the XMP datacenter, which supports all workloads from the AMP-VX and all VxBlock Systems. This can be named to identify a datacenter location or provide a
unique name to this AMP-VX environment (for example, NYC1-XMP). It is possible to include multiple VMware vSphere ESXi datacenters in a single AMP-VX instance with multiple VMware vSphere ESXi clusters.

- **VMware vSphere Cluster:** One VMware vSphere cluster in the VMware vCenter Server accommodates the AMP-VX core, optional workloads, and AMP-VX ECO workloads. A minimum of four servers per cluster is required to provide the performance and resiliency features of VMware vSAN.

- **Folders:** The following folders are assigned to each type of workload to organize the AMP-VX and VxBlock System management applications.
  - **AMP-VX_mgmt:** Contains the VMs that support the AMP-VX VMware vCenter Server and jump server. This folder contains a child folder to separate the local element manager VMs (AMP-VX_local) from the VMware vCenter Server environment.
  - **Prod_mgmt:** Contains the VMs that support the VMware vCenter Server environment, element manager and Vision Intelligent Operations or VxBlock Central. This folder contains child folders to further separate the VMware vCenter Server environment (XMP_Prod_Central) from the element managers (XMP_Prod_Cmn). XMP_Prod_Central contains a sub-folder for each instance of VxBlock System VMware vCenter Servers:
    - **XMP_Prod01:** Contains the first production shared management VMware vCenter Server VMs.
    - **XMP_Prod02:** Contains an additional production shared management VMware vCenter Server VMs.
  - **XMP_Prod_Cmn:** Contains sub-folders to separate element managers common across all VxBlock Systems, including AMP-VX:
    - **XMPcmn01:** Provides the shared managed VMs that support XMP Vision software or VxBlock Central, Element Manager, Secure Remote Services, Cisco DCNM, and PowerPath across all VxBlock Systems. If desired, more than one XMPcmnxx can be configured to separate the management VMs for each VxBlock System. This vAPP is a member of the XMP_Prod_Cmn folder.
    - **Opt_mgmt:** Contains VMs that support the optional components for VxBlock Systems.
    - **Eco_mgmt:** Contains VMs that support the ecosystem workloads for VxBlock Systems.

**Management workloads (VMware vSphere 6.x)**

The AMP supports core management workload, Dell EMC optional management workload, and ecosystem workloads.

**Core management workloads (VMware vSphere 6.7)**

The core management workload consists of the AMP-VX and VxBlock Systems management VMware vCenter Servers. Together, the management VMware vCenter Servers contain both AMP-VX management and production shared management workloads. Core workloads are required to manage AMP-VX and VxBlock Systems.

Both workloads are split up into folders under the XMP-CORE cluster:

- **AMP-VX_mgmt:** Manages the local components for AMP-VX. The AMP-VX management folder contains the local workloads for the VMware vSphere management components that run the AMP-VX.
- **Prod_mgmt:** This folder is used for all VxBlock Systems. The production management folder contains the following:
  - The central/shared workloads for the VMware vSphere management components
  - The common components, such as Cisco Element Manager, Secure Remote Services, Cisco DCNM, and PowerPath

The shared and common workloads are further separated as subfolders of the production shared management folder. The following table provides the servers that belong in AMP-VX and production shared management folders:
<table>
<thead>
<tr>
<th>Folder</th>
<th>Includes</th>
<th>Manages</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMP-VX_mgmt</td>
<td>AMP-VX VMware vCenter Server with Embedded PSC (default)</td>
<td>AMP-VX system components</td>
</tr>
<tr>
<td></td>
<td>AMP-VX VMware vCenter Server with External PSC 1 (optional)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AMP-VX VMware vCenter Server with External PSC 2 (optional)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> VMware vSphere 6.7 and VMware vSphere 6.5 are the last VMware vSphere releases that support the deployment of external PSCs. Updates to both of these VMware vSphere versions support Enhanced Linked Mode in embedded PSCs, making external PSCs no longer necessary. Upgrading to VMware vSphere 6.7 update 1 or VMware vSphere 6.5 update 2d enables you to migrate external PSCs to embedded PSCs. For more information about changing to embedded PSCs from external PSCs, consult with your account team.</td>
<td></td>
</tr>
<tr>
<td>Prod_mgmt</td>
<td>Production VMware vCenter Server with Embedded PSC (default)</td>
<td>Managed VxBlock System resources</td>
</tr>
<tr>
<td></td>
<td>Production VMware vCenter Server with External PSC 1 (optional)</td>
<td>(including storage, compute, virtualization, and network)</td>
</tr>
<tr>
<td></td>
<td>Production VMware vCenter Server with External PSC 2 (optional)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Production Element Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Production Cisco DCNM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Production Secure Remote Services appliance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Production PowerPath License</td>
<td></td>
</tr>
</tbody>
</table>

**Optional management workload**

The Dell EMC optional management workload consists of all the optional software components that are not required components of the VxBlock System.

The \texttt{Opt_mgmt} folder resides under VMware vSphere Cluster, XMP-CORE.

**Ecosystem management workload (VMware vSphere 6.x)**

The ecosystem management workload consists of non-Dell EMC engineered management tools from Cisco, Dell EMC, and VMware, as well as software certified as VxBlock System-ready, such as VMware vRealize Suite, VMware Horizon View, Cisco UCS Director, ViPR, VMware VMTurbo, and BMC Cloud Lifecycle Management.

\texttt{Eco_mgmt} is created under the VMware vSphere Cluster, XMP-Core. To segregate this workload from the other workloads, it may be created on a separate AMP-VX.
Manage the AMP (VMware vSphere 6.7)

Vision Intelligent Operations or VxBlock Central and VMware vRealize Log Insight software are used to manage AMP-VX.

VxBlock Central

VxBlock Central is available in the following options:

- The Base option provides the VxBlock Central user interface.
- The Workflow Automation option adds VxBlock Central Orchestration, which provides:
  - VxBlock Central Orchestration Services
  - VxBlock Central Orchestration Workflows
- The Advanced Analytics option adds VxBlock Central Operations and VxBlock Central Orchestration.

The VxBlock Central dashboard provides system inventory, health monitoring, and RCM compliance management. VxBlock Central also includes the VxBlock Central Shell shell, which provides network configuration and other capabilities necessary for management.

VxBlock Central provides the ability to:

- View the health and RCM compliance of multiple VxBlock Systems.
- View charts of key performance indicators (KPI) for one or more components or elements.
- Download software and firmware to maintain compliance with the current RCM.
- Track critical faults, errors, and issues affecting VxBlock Systems.
- Configure multisystem AD integration and map AD Groups to VxBlock Central roles.
- Set up compute, storage, networks, and PXE services, manage credentials, and upload ISO images for server installation.
- Monitor VxBlock System analytics and manage capacity through integration with VMware vRealize Operations (vROps).

Dell EMC recommends using VxBlock Central as your primary management interface.

VMware vRealize Log Insight software

VMware vRealize Log Insight software provides log analytics. VMware vRealize Log Insight is the syslog server for AMP-VX including all components, hosts, VMware vCenter and production VMware vCenter servers. Any VM running on the servers can also use VMware vRealize Log Insight as their syslog server.

Use VxBlock Central as the SNMP trap collector for AMP-VX and VxBlock Central components.

For more information about VMware vRealize Log Insight, see Installing and Configuring vRealize Log Insight at VMware Docs.

Management software components (VMware vSphere 6.x)

The AMP is delivered with specific installed software components dependent on the selected RCM.

The following components are installed as part of the base configuration:

- VxBlock Central
- Microsoft Windows
- VMware vSphere Enterprise Plus
Configure system monitoring (VMware vSphere 6.x)

Configure system monitoring for the AMP-VX server using the iDRAC interface.

Before you begin
Verify access to the iDRAC interface.

Procedure

1. Log in to the iDRAC interface of the node.
2. Select Configuration > System Settings > Alerts or Alert: Configuration and confirm Enabled is selected. If not, select Enabled and click Apply.
3. Under Alerts and Remote System Log Configuration, select the alerts to enable and click Apply.
4. Select the SNMP Traps Configuration tab.
   
   Note: The community string should already be populated for the software server and should not be removed.

5. To add a second destination IP address for an existing monitoring system, type the address into the Alert Destination2 IP field, check State and click Apply.
   
   Note: Monitoring must support SNMP v2 and use the community string configured on the AMP-VX server for Vision software or VxBlock Central.

6. Under Destination Email Addresses, for each parameter, type the following:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Alert 1-4</td>
<td>email address to send the alert.</td>
</tr>
<tr>
<td>Primary SMTP (email) server IP address or FQDN /DNS Name</td>
<td>IP address associated with the primary SMTP server to which email is sent.</td>
</tr>
</tbody>
</table>
Enable Authentication | Check this box if the SMTP server requires SMTP authentication. This also enables setting the username and password.
Username | Type the username which is part of the authentication credentials for the primary SMTP server. Used only if authentication is enforced.
Password | Type the password which is part of the authentication credentials for the primary SMTP server. Used only if authentication is enforced.
SMTP port number | If an SMTP port other than 25 is used (for example, 587).

7. Click Apply.

Manage VMware vSphere operations (VMware vSphere 6.7)
Use the VMware vSphere client to perform management tasks on AMP-VX.
The following table provides the management tasks you can perform with the VMware vSphere client:

<table>
<thead>
<tr>
<th>Management task</th>
<th>Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage servers and hosts</td>
<td>vCenter Server and Host Management</td>
</tr>
<tr>
<td>Administer VMware vSphere</td>
<td>vSphere Administration with the vSphere Client</td>
</tr>
</tbody>
</table>

- Monitor VMware vSAN.

Related information
VMware vSphere 6.7 Documentation Center

Monitor VMware vSAN (VMware vSphere 6.7)
Monitor VMware vSAN on the AMP-VX.

About this task
Exercise caution when accessing the AMP-VX VMware vCenter Server. Do not make any configuration changes other than those documented because it may result in loss of monitoring and remote support capabilities.

Procedure
1. Launch the VMware vSphere HTML5 client, type the username and password and log in.
2. Click Hosts and Clusters.
3. Select the cluster hosting the AMP-VX servers.
4. Select Monitor > vSAN > Health.
5. Verify that all tests pass. If Warning or Failed displays, investigate and troubleshoot the cause.

Prepare the VMware vSphere ESXi server for temporary maintenance (VMware vSphere 6.7)
Follow specific instructions for VMware ESXi hosts using VMware vSAN software-defined storage before performing maintenance activities.

About this task
Do not use this procedure if the server must be offline for a long period of time or if it will be powered off.
Procedure
1. Log in to the VMware vCenter Server and select Hosts and Clusters.
2. Locate and right-click the VMware vSphere ESXi host, and select Maintenance Mode > Enter Maintenance Mode.
3. Verify Ensure data accessibility from other hosts is checked.
4. Monitor tasks in Recent tasks.
5. Verify the host is in Maintenance Mode in the Navigator window.

Prepare the VMware vSphere ESXi server for shutdown (VMware vSphere 6.7)
When preparing a server shutdown for system hardware maintenance, VMware ESXi hosts using VMware vSAN software-defined storage require specific instructions to be followed.

Procedure
1. Log in to VMware vSphere client (HTML5) and select Hosts and Clusters.
2. Locate the VMware vSphere ESXi host to shut down.
3. Right-click the VMware vSphere ESXi host, and select Maintenance Mode > Enter Maintenance Mode.
   a. Verify Move powered-off and suspended virtual machines to other hosts in the cluster is checked.
   b. Select Evacuate all data to other hosts and click OK.
   c. Monitor tasks in Recent tasks.
   d. Validate the host is in Maintenance Mode in the Navigator window.
4. Right-click the VMware vSphere ESXi host and select Actions > Power > Shut down.

Boot the VMware vSphere ESXi host (VMware vSphere 6.7)
Boot the VMware vSphere ESXi host from the iDRAC interface.

Procedure
1. Log in to the iDRAC interface.
2. From the main dashboard, select Power on System and click OK.
3. Monitor power up from the Dashboard Virtual Console window or launch the virtual console.
4. When VMware vSphere ESXi has finished loading, log in to the VMware vCenter Server.
5. Navigate to Hosts and Clusters.
6. Validate the host is in Maintenance Mode and the following message does not open:

   not responding

   Note: Refresh the VMware vCenter Server window if necessary.
7. Right-click the serviced host and select Maintenance Mode/Exit Maintenance Mode.
8. Monitor recent tasks for completion.
9. To validate VMware vSAN health, perform the following steps:
   a. Select the AMP-VX Cluster, then select Monitor tab, the vSAN subtab, and the Health menu item.
   b. Select Retest.
c. Look for any warnings and run recommended steps.

   Note: Procedures that slow or consume excessive resources should be run during maintenance hours only. For example, Proactive Rebalance Disks should be run during a maintenance window.

d. If there is a warning on Cluster - vSAN Disk Balance, select Proactive Rebalance Disk.

e. Navigate to Host and Clusters.

f. Select XMP-Core cluster (the cluster name may be different).

g. Select the Configure tab and select vSAN/Disk Management.

h. Select the host from the top window.

i. Verify the following:
   - Five of five disks are in use, connected, and healthy.
   - One disk group is mounted, healthy, and all flash.
   - Five healthy and mounted disks are listed in the bottom window, all flash:
     - one cache disk
     - four capacity disks

10. Navigate to Hosts and Clusters and select a host.

11. Select Hosts > Configuration > Datastore.

12. Verify the VMware vSAN datastore device is listed as a datastore on the host.

After you finish

For more information, see Dell EMC Converged System Powering On and Off Guide.

Install the latest VMware vSphere ESXi patch (VMware vSphere 6.7)

After the latest patch is installed, when you update a VMware vSphere ESXi host to a newer supported build, the host no longer shares the same build.

About this task

Use the VMware vSphere Update Manager (VUM) if upgrading to a newer supported build. You can use the CLI to install the patch. Do not use this procedure for major upgrades.

Before you begin

- Verify AMP-VX iDRAC, hosts, VMware vSphere environment, and VMware vSAN health check have no warnings or errors. Correct any warnings or errors before proceeding with the upgrade.
- Verify that the host is in Maintenance mode.
  - Select Move powered-off and suspended virtual machines to other hosts in the cluster.
  - Select Evacuate all data to other hosts and select OK.
- Only a single AMP-VX host can be placed into maintenance mode at a time.
- AMP-VX host software upgrades must be sequential.
- Verify software compatibility for the following:
  - AMP-VX Dell PowerEdge servers BIOS firmware
  - iDRAC firmware
  - HBA 330 mini driver firmware
Mellanox adapter firmware
Intel X550 firmware
The build to which you are upgrading

**Note:** You may need to upgrade third-party software prior to updating to the latest release of VMware vSphere ESXi.

- Obtain the *Release Certification Matrix* and *Release Notes* with the version to which you want to update.
  - Look for the supported version of the VMware patch (build) in the *Virtualization* section.
  - Determine which patch to install

**Procedure**

1. Download the latest VMware vSphere ESXi patch supported for this release.
2. Using a browser, go to the download center on the Support.
3. Select and download the latest supported VMware vSphere ESXi patch.
4. Install the patch as described in *VMware knowledge base article 2008939*.
5. To verify the installation, on the VMware vSphere ESXi host, confirm that the build number matches the update that is just applied.
6. Reboot the VMware vSphere ESXi host.
7. After the host reboots, remove the host from maintenance mode.
8. Verify AMP-VX iDRAC, hosts, VMware vSphere environment, and VMware vSAN health check have no warnings or errors. Correct any warnings or errors before proceeding with upgrades of the remaining AMP-VX hosts.

**Related information**

- VMware Knowledge Base
- Support

### Patch VMware vSphere ESXi hosts with the VMware vSphere Update Manager (VMware vSphere 6.7)

When a new VMware vSphere ESXi host is deployed or requires an update, patch VMware vSphere ESXi hosts with the VMware vSphere Update Manager (VUM) with the HTML5 client.

**Before you begin**

- Verify that the patch bundle is listed on the latest version of the *Converged Systems Release Certification Matrix*.
- Verify the software compatibility for the AMP-VX components listed on the RCM. You may need to upgrade third-party software prior to updating to the latest release of VMware vSphere ESXi.
- Verify AMP-VX iDRAC, hosts, VMware vSphere environment, VMware vSAN health check have no warnings or errors.
  - Correct any warnings or errors before proceeding with the upgrade.
  - Only a single AMP-VX host can be placed into maintenance mode at a time.
  - AMP-VX host software upgrades must be sequential.

**Procedure**

1. Log in to VMware vSphere HTML5 client.
2. Right-click the VMware vSphere ESXi host and select **Maintenance Mode > Enter Maintenance Mode**
3. Select **Move powered-off and suspended virtual machines to other hosts in the cluster**.
4. Select **Evacuate all data to other hosts** and click OK.
Note: Do not place more than one AMP-VX host at a time in maintenance mode. AMP-VX VMware VUM host upgrades must be sequential. This allows VMware vCenter Server and the AMP-VX VMware vSAN cluster to continue to operate.

5. In the VMware vSphere client (HTML5), select the host and select the Updates tab.
6. In the Updates page, click the Update Manager Home button.
7. From the Update Manager page, click Updates > UPLOAD FROM FILE.
8. In the Import Patches window, click Browse.
9. Browse to the location of the saved patch file or package software bundle, select the file, and click Open.
10. Click Next and wait until the file upload completes successfully.
    If the upload fails, the zip file may have been corrupted during the download process or the incorrect zip file has been imported. Try downloading the zip file again and then import.
11. Click Next.
12. From the Import Patches wizard on the Ready to complete page, verify the package that you imported into the VMware VUM repository and click Finish.
13. In the ADD/REMOVE BASELINES pane, verify that the patch appears in the list.
14. Select the Baselines tab and click New > Baseline to create a new baseline.
15. In the Baseline Definition wizard:
    a. In the Name field, type the package name. For example, HBA330.
    b. For the Content, select Patch and click Next.
    c. Click the Matched tab.
    d. In the Patches to Exclude window, exclude all patches except HBA330.
    e. In the Add Patches manually window, click Next and Finish.
16. Attach the package baseline to the desired VMware vSphere ESXi hosts. You can attach the package baseline to individually selected VMware vSphere ESXi hosts or to multiple hosts by selecting the cluster in the Inventory > Hosts and Clusters view.
17. To attach the package baseline to an individual VMware vSphere ESXi host, highlight the desired host in the Hosts and Clusters list and select the Updates tab.
18. To attach the package baseline to several VMware vSphere ESXi hosts, perform the following steps:
    a. In the left-side list, select a folder, cluster, or datacenter.
    b. In the right window, select the Updates tab and then select Host Updates.
    c. In the Attach Baselines window, select the package baseline that was previously created and click ATTACH.
    d. From the Attach list, select the baseline and click ATTACH.
19. Go to Overview and click CHECK COMPLIANCE under Hosts’ Compliance.
20. Go to Host Updates and check the Compliance Status for the attached baseline. If the status is non-compliant, remediate (patch) the host using the patches in the baseline.
21. Staging is the process of pushing the package onto individual VMware vSphere ESXi hosts from the VMware VUM server. To stage the baseline, perform the following:
    a. In the Updates section, select the package baseline that was created in the Baselines list under Attached Baselines.
    b. Click STAGE.
    c. When the Stage Patches Wizard appears, under Install in the Baselines list, verify that the package baseline that was created is selected.
d. In the Hosts pane, all the VMware vSphere ESXi hosts to which the package baseline is attached are selected by default. If required, alter the default Host selection to stage the baseline to only one or some of the VMware vSphere ESXi hosts and click OK.

e. In the Patch and Extension Exclusion window, verify package information and click Next.

f. When the Ready to Complete window appears, verify the information and click Finish.

22. During remediation, packages are installed on hosts that do not have the package and/or the package is updated on hosts that have an outdated package. To remediate the baseline, perform the following steps:

a. Highlight the VMware vSphere ESXi host to remediate and select the Updates tab.

b. In the Host Updates section, under Attached Baselines, select the package baseline that was created and click Remediate.

c. In the Remediate window, review the remediation pre-check report and address any issues. All of the VMware vSphere ESXi hosts to which the package baseline is staged are selected by default.

d. Click REMEDIATE to remediate the host.

23. After VMware VUM has completed patching the ESXi host, remove the host from maintenance mode.

24. Verify AMP-VX iDRAC, hosts, and VMware vSphere environment have no warnings or errors. Verify VMware vSAN health check does not have any warnings or errors. Correct any warnings or errors before proceeding with any further host upgrades.

25. To proceed with the upgrade of the remaining AMP-VX hosts, perform the following steps:

a. Right-click the VMware vSphere ESXi host and select Maintenance mode > Enter Maintenance Mode.

b. Select Move powered-off and suspended virtual machines to other hosts in the cluster.

c. Select Evacuate all data to other hosts and click OK.

Go to Overview and click CHECK COMPLIANCE under Hosts' Compliance.

Go to Host Updates and check the Compliance Status for the attached baseline. If the status is non-compliant, remediate (patch) the host using the patches in the baseline.

Note: With AMP-VX, do not place more than one AMP-VX host at a time in maintenance mode.

d. Repeat Step 21 for each remaining AMP-VX host to be upgraded.

Manage VMware Single Sign On (VMware vSphere 6.x)

VMware vCenter Single Sign On (SSO) is an authentication mechanism used to configure security policies and lock out or disable an account for VMware vSphere 6.x.

Default policies do not require modification. You may have to modify policies or accounts if regulations require different policies or when troubleshooting a problem.

Unlock and reset the VMware Single Sign On administrator password (VMware vSphere 6.x)

The VMware vSphere knowledge base article KB 2034608 contains instructions to unlock a VMware Single Sign On (SSO) administrator account.

About this task

For security purposes, the VMware vCenter administrator account is locked after three failed attempts to log in.

Procedure

1. Follow the procedure in the VMware knowledge base article 2034608.
Manage the lockout status of VMware Single Sign On (VMware vSphere 6.x)

View the lockout status of a VMware Single Sign On (SSO) account for VMware vSphere.

About this task
By default, the VMware SSO administrator username is administrator@vsphere.local.

Procedure
1. Depending on which version of VMware vSphere 6.x you are running, perform one of the following:
   - For VMware vSphere 6.7, log in to the VMware vSphere HTML5 Client as administrator@vsphere.local.
   - For VMware vSphere 6.5, log in to the VMware vSphere Web Client as administrator@vsphere.local.
2. From the home page, select Administration > Single Sign-On > Users and Groups.
3. Each tab shows information from the identity sources about configured accounts on the system. Select the Users tab.
4. The Locked or Disabled columns show the status of each configured VMware SSO account. In VMware vSphere HTML5 Client, click the ellipsis-vertical bar near the user to Enable/Disable or Unlock.
   
   Note: The Locked Users and Disabled Users tabs provide information for the identity sources only.
5. Click Yes to confirm.

Manage VMware Single Sign On default password policies (VMware vSphere 6.x)

Manage the VMware Single Sign On (SSO) default password policies for VMware vSphere.

About this task
By default, the VMware SSO passwords expire after 90 days, including the VMware SSO administrator password. You can modify the expiration policy.

Procedure
1. Depending on which version of VMware vSphere 6.x you are running, perform one of the following:
   - For VMware vSphere 6.7, log in to the VMware vSphere HTML5 Client as administrator@vsphere.local.
   - For VMware vSphere 6.5, log in to the VMware vSphere Web Client as administrator@vsphere.local.
2. From the home page, select Administration > Single Sign-On > Configuration.
4. To modify the password policy, click Edit.
5. Make the required changes and click OK.

Manage VMware Single Sign On lockout policies (VMware vSphere 6.x)

Modify the strict lockout policy of VMware Single Sign On (SSO) for VMware vSphere 6.x.

Procedure
1. Depending on which version of VMware vSphere 6.x you are running, perform one of the following:
   - For VMware vSphere 6.7, log in to the VMware vSphere HTML5 Client as administrator@vsphere.local.
   - For VMware vSphere 6.5, log in to the VMware vSphere Web Client as administrator@vsphere.local.
2. From the home page, select Administration > Single Sign-On > Configuration.
3. Select the Policies tab and then select Lockout Policy to view the current lockout policies.
4. To modify the lockout policy, select Edit.
5. Make required changes and click OK.

Add an AD identity source to VMware Single Sign On (VMware vSphere 6.7)

Associate Windows AD to the VMware Single Sign On (SSO) service for VMware vSphere 6.7 on the VMware Platform Services Controllers (PSCs).

**Before you begin**

Obtain network access to the VMware vCenter HTML5 Client and use AD domain admin privileges.

**Procedure**

1. Log in to the VMware vSphere 6.7 HTML5 Client using the administrator@vsphere.local account at: https://<vcenter_fqdn or ip>/ui/
2. Select Menu > Administration.
4. For embedded VMware PSC deployment, select vCenter server with Embedded PSC and click Join AD.
5. Type the AD domain, username, and password (with appropriate AD domain administrative rights). Leave Organizational unit blank and click OK.
6. Leave Organizational unit blank and click OK.
7. Reboot the node.

**Note:** VMware vSphere 6.7 and VMware vSphere 6.5 are the last VMware vSphere releases that support the deployment of external PSCs. Updates to both of these VMware vSphere versions support Enhanced Linked Mode in embedded PSCs, making external PSCs no longer necessary. Upgrading to VMware vSphere 6.7 update 1 or VMware vSphere 6.5 update 2d enables you to migrate external PSCs to embedded PSCs. For more information about changing to embedded PSCs from external PSCs, consult with your account team.

   a. Select the VMware PSC to join to the AD domain and click JOIN AD.
   b. Leave Organizational unit blank and click OK.
   c. As root, log in to https://<psc_fqdn>:5480/.
   d. Restart the appliance.
   e. Repeat these steps for each PSC.
9. Select the Identity Sources tab and click ADD IDENTITY SOURCE to enter details for the AD domain being added.
10. Select the Active Directory (Integrated Windows Authentication) under Identity source type.
11. Verify that the domain name was previously registered to the VMware PSC is assigned to this AD domain registration.
12. Click Use machine account > OK.
13. Select the added AD domain and Click SET AS DEFAULT.
Assign Administrator roles and permissions for domain user accounts or groups that require access to VMware vCenter 6.7. By default, only the administrator@vsphere.local account can access VMware vCenter Server until more permissions are explicitly assigned to domain users.

Install VMware vCenter Server root certificates on a web browser (VMware vSphere 6.x)

Install trusted root certificates on Internet Explorer only. For browsers other than Internet Explorer, see browser documentation.

Procedure
1. Open Internet Explorer and go to https://vcsa_fqdn.
2. From the VMware vCenter Server getting started page, select Download trusted root CA certificates and save the file locally.
3. Unzip the downloaded files.
4. Right-click each .crt file and click Open.
5. In the pop up dialog click Install Certificate.

Exact steps may vary depending on the version of the browser. For additional information, see VMware Knowledge Base article 2108294.

Related information
VMware Knowledge Base

Redirect VMware vCenter Server to the secondary external VMware Platform Services Controller (VMware vSphere 6.x)

For VMware vSphere 6.x, repoint the VMware vCenter Server for authentication under the following conditions: the primary external VMware Platform Services Controller (PSC) fails, there are multiple VMware PSCs replicating, and the PSCs are configured without fault tolerance.

Note: VMware vSphere 6.7 and VMware vSphere 6.5 are the last VMware vSphere releases that support the deployment of external PSCs. Updates to both of these VMware vSphere versions support Enhanced Linked Mode in embedded PSCs, making external PSCs no longer necessary. Upgrading to VMware vSphere 6.7 update 1 or VMware vSphere 6.5 update 2d enables you to migrate external PSCs to embedded PSCs. For more information about changing to embedded PSCs from external PSCs, consult with your account team.

See the Repointing the Connections Between vCenter Server and PSC section of the VMware vSphere Installation and Setup Guide.

Related information
VMware docs
Network (VMware vSphere 6.5)

VxBlock System 1000 offer several types of management network connectivity and server assignments. The AMP-VX connects to the management and data switches included in the VxBlock 1000.

AMP-VX servers connect to the ToR switches with 1 x dual port + NICs (one port per switch) to communicate with in-band components of the infrastructure. Depending on the capability of the switch, the connection is either + direct connect cable or + using breakout cables.

AMP-VX connects to the VxBlock 1000 management network switches using:

- 4 x 10-GbE Base-T ports for VMware vSAN, management data, and out of band components
- One 10-GbE Base-T port for the iDRAC connection for remote management of each AMP-VX server

Three ports connect to one switch (iDRAC and one VMware vSAN and one management port), two ports connect to the other switch (one VMware vSAN and one management port) with the original standard switch model.

The following diagram shows VMware vSphere ESXi network connectivity on AMP-VX servers with VMware standard switches:
Two ports connect to one switch (for iDRAC, VMware vSAN and management) and one port connects to the other switch (for VMware vSAN and management) with the VMware vSphere Distributed Switch (VDS) model.

The following diagram shows VMware vSphere ESXi network connectivity on AMP-VX M5 servers with the VMware VDS:
See the *Dell EMC VxBlock System 1000 Architecture Overview* to understand specific network switch capabilities.

For information about VMware NSX 6.4 with the VxBlock System 1000 and AMP-VX, see the *Dell EMC VxBlock™ System 1000 for VMware NSX 6.4 Architecture Overview*.
Network architecture and design (VMware vSphere 6.5)

Most network connectivity between components in a VxBlock System is internal. In AMP-VX, management network connectivity is accessible to any AMP-VX managed VxBlock System.

Layer 2 or Layer 3 routing (default) is configured between the management plane and the external network to enable management functionality. These routing configurations are implemented at the management or management aggregation switches.

For L2 traffic, AMP-VX VLANs remain local to the management plane of the VxBlock System. AMP-VX uses VMware vSphere Standard Switch or VMware vSphere Distributed Switches (VDS) as its virtual networking switch.

The logical network design for AMP-VX reduces impact from network outages. The design optimizes the environment for advanced security implementations, such as Dell EMC secure administrative access and trusted multitenancy solutions. The VLAN design is similar to a standard VxBlock System.

AMP-VX uses the following types of networking:

- In-band management
- Out-of-band management
- Inter-VxBlock System
- Virtual

**In-band management networking**

The in-band management networking traverses the ToR network switches within the VxBlock System.

The following table shows VLANs that carry management traffic local to the VxBlock System:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcesys_esx_mgmt</td>
<td>VxBlock System VMware management and applications that may impact production.</td>
</tr>
<tr>
<td>vcesys_esx_vmotion</td>
<td>VMware vSphere vMotion L3 traffic between VxBlock System VMware vSphere ESXi hosts.</td>
</tr>
<tr>
<td>vcesys_esx_ft</td>
<td>VMware fault tolerance traffic between VxBlock System VMware vSphere ESXi hosts.</td>
</tr>
<tr>
<td>vcesys_brs_data</td>
<td>Backup and recovery with data protection solution.</td>
</tr>
<tr>
<td>vcesys_nfs</td>
<td>NAS VLAN</td>
</tr>
<tr>
<td>vcesys_esx_build</td>
<td>VLAN required for VM deployment.</td>
</tr>
</tbody>
</table>

The vcesys_esx_vmotion and vcesys_nfs VLANs remain local (and internal) to each managed VxBlock System and are not routed through the core network.

The following table shows the AMP-VX in-band VLANs local to AMP-VX that traverse the ToR switches:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>amx_esx_mgmt</td>
<td>AMP-VX VMware management and applications.</td>
</tr>
<tr>
<td>amx_esx_vmotion</td>
<td>VMware vSphere vMotion L3 traffic between AMP-VX VMware vSphere ESXi hosts.</td>
</tr>
<tr>
<td>amx_esx_ft</td>
<td>VMware fault tolerance traffic between AMP-VX VMware vSphere ESXi hosts.</td>
</tr>
</tbody>
</table>

There are two AMP-VX in-band management VLANs that traverse the VxBlock System management switches. AMP-VX in-band management network does not impact production use of the VxBlock System.

VMware vSphere ESXi VLANs that carry management traffic local to AMP-VX may not be used for any production data.

The following table shows the VMware vSphere ESXi VLANs that carry management traffic local to AMP-VX:
### VLANs

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>amx_esx_mgmt</td>
<td>AMP-VX VMware management applications for the standard switch.</td>
</tr>
<tr>
<td>amx_esx_vmotion</td>
<td>VMware vSphere vMotion L3 traffic between AMP-VX VMware vSphere ESXi hosts for the standard switch.</td>
</tr>
<tr>
<td>amx_esx_ft</td>
<td>VMware fault tolerance traffic between AMP-VX VMware vSphere ESXi hosts for the standard switch.</td>
</tr>
<tr>
<td>amx_esx_build</td>
<td>VLAN required for VM deployment on AMP-VX for the standard switch.</td>
</tr>
<tr>
<td>amx_brs_data</td>
<td>AMP-VX backup and recovery with Integrated Data Protection solution.</td>
</tr>
</tbody>
</table>

The **amx_esx_vmotion** and **amx_esx_ft** VLANs remain local (and internal) to the AMP-VX and are not routed through the core network.

### Out-of-band management networking

Out-of-band networks do not impact production use of the VxBlock System. This traffic traverses the management switches within the VxBlock System.

The following table shows the networks that may not be applied for any production data:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcesys_ipmi</td>
<td>Used for Data Domain IPMI. There is no data on this VLAN.</td>
</tr>
<tr>
<td>vcesys_oob_mgmt</td>
<td>VMs and device ports are used for control plane only by both the VxBlock System and the AMP-VX. There is no data on this VLAN.</td>
</tr>
<tr>
<td>amx_vsan</td>
<td>Used for AMP-VX VMware vSAN cluster network communication.</td>
</tr>
</tbody>
</table>

The **amx_vsan** VLAN remains local (and internal) to the AMP-VX and is not routed through the core network.

### Inter-VxBlock System networking

The following VLANs provide network connectivity to the VxBlock System or to the external management and production networks for consumption with VMware standard switches:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>xmp_vceopt_mgmt</td>
<td>Dell EMC optional management workload VMs (may be collapsed into core).</td>
</tr>
<tr>
<td>xmp_eco_mgmt</td>
<td>Ecosystem management workload VMs.</td>
</tr>
</tbody>
</table>

### Virtual networking

The following table describes production and management VLANs:
<table>
<thead>
<tr>
<th>VLAN</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcesys_esx_mgmt</td>
<td>Carries inter-VxBlock System management traffic to and from the VMs in the XMP_Prod_Central management workload folder. The following specifications should be considered for this VLAN:</td>
</tr>
<tr>
<td></td>
<td>• If L2 network connectivity is required, use a /22 subnet or larger to accommodate IP addressing for from 650 to 2,000 VMware vSphere ESXi hosts.</td>
</tr>
<tr>
<td></td>
<td>• If L3 network connectivity is required, size the assigned subnet according to the number of VMs supporting the managed VxBlock System. Plan the subnet size to include 3 VMs per VMware vCenter instance.</td>
</tr>
<tr>
<td></td>
<td>• L2 or L3 connectivity through the customer-provided network is required to establish management functionality between the AMP-VX and managed VxBlock System.</td>
</tr>
<tr>
<td>vcesys_oob_mgmt</td>
<td>Carries inter-VxBlock System management traffic to and from the VMs in the XMP_Prod_Cmn_rp management workload folder. The following specifications should be considered for this VLAN:</td>
</tr>
<tr>
<td></td>
<td>• If L2 network connectivity is required, use a /22 subnet or larger to accommodate for IP addressing for from 650 to 2,000 VMware vSphere ESXi hosts.</td>
</tr>
<tr>
<td></td>
<td>• If L3 network connectivity is required, ensure to size the subnet to accommodate all management VMs, KVMs, and system components requiring out of band management.</td>
</tr>
<tr>
<td></td>
<td>• L2 or L3 connectivity through the customer-provided network is required to establish management functionality between the AMP-VX and managed VxBlock System.</td>
</tr>
<tr>
<td>xmp_vceopt_mgmt</td>
<td>Carries inter-VxBlock System management traffic to and from the VMs in the optional management workload VMware vSphere cluster folder. The following specifications should be considered for this VLAN:</td>
</tr>
<tr>
<td>(for standard switches)</td>
<td>• If L2 network connectivity is required, use a /22 subnet or larger to accommodate for IP addressing for the following:</td>
</tr>
<tr>
<td></td>
<td>▪ 650-2,000 VMware vSphere ESXi hosts</td>
</tr>
<tr>
<td></td>
<td>▪ The necessary Dell EMC optional management workload VMs</td>
</tr>
<tr>
<td></td>
<td>• For L3 network connectivity, size the assigned subnet to accommodate the required number of VMs to support the Dell EMC optional management workload VMs.</td>
</tr>
<tr>
<td></td>
<td>• L2 or L3 connectivity through the customer-provided network is required to establish management functionality between the AMP-VX and managed VxBlock Systems.</td>
</tr>
<tr>
<td>xmp_eco_mgmt</td>
<td>Carries inter-VxBlock System management traffic to and from the VMs in the ecosystem management workload folder. The following specifications should be considered for this VLAN:</td>
</tr>
<tr>
<td>(for standard switches)</td>
<td>• IP address and subnet allocations for L2 and/or L3 network connectivity are client that is specified to meet the ecosystem management workload application requirements.</td>
</tr>
<tr>
<td></td>
<td>• L2 or L3 connectivity through the customer-provided network is required to establish management functionality between the AMP-VX and managed VxBlock Systems.</td>
</tr>
</tbody>
</table>

The following figure shows an example of VLAN requirements and usage for AMP-VX and VxBlock Systems using VMware standard switches (Embedded PSC):
The following figure shows an example of VLAN requirements and usage for AMP-VX and VxBlock Systems using VMware standard switches (External PSC):
Note: Not all management applications are shown in this diagram.

The following figure shows an example of VLAN requirements and usage with VxBlock Central and VMware VDS (Embedded PSC):
The following figure shows an example of VLAN requirements and usage with VxBlock Central and VMware VDS (External PSC):
Inter-VxBlock System connectivity use case (VMware vSphere 6.5)

The AMP-VX network architecture allows for a Layer 3 scenario to establish inter-VxBlock System connectivity. The host AMP-VX system must be in the same data center or within a metro 10 ms R/T latency distance of the VxBlock Systems.

The following table provides an L3 use case, requirements, and caveats:

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L3</td>
<td>Inter-VxBlock System connectivity using L3 capability.</td>
</tr>
</tbody>
</table>

Description

This option uses L3 routing between the AMP-VX VLANs and the VxBlock System VLANs for management traffic.
### Use Case Requirements

The following management networks residing on the VxBlock System as well as the AMP-VX management VLANs must have L3 routing configuration implemented.

- `vcesys_esx_mgmt`
- `vcesys_oob_mgmt`
- `amx_esx_mgmt`

This enables management functionality between the AMP-VX and the managed VxBlock Systems.

`vcesys_oob_mgmt` requires L3 routing to access applications running on management VMs that reside on the out-of-band network. `vcesys_esx_vmotion` (vMotion Netstack) and `vcesys_nfs` remain local (and internal) to each of the managed VxBlock Systems and are not routed through the core network.

The following illustration provides sample L3 routing configurations required on the core network layer using VMware VDS:
Virtual networking (VMware vSphere 6.5)

AMP-VX includes virtual networking standards that allow each VM to connect to the physical network. Deploy the virtual networking components on the AMP-VX and place them in a manner to support a maximum level of redundancy (where choices are available).
VMware vSphere Standard Switch design (VMware vSphere 6.5)

The AMP-VX VMware ESXi host has VMKernel, VM port groups, and vMotion configured on the same VMware vSphere Standard Switch as out-of-band management.

VMware vSAN is configured on a second VMware vSphere Standard Switch. The AMP-VX ESXi hosts are managed by the AMP-VX VMware vCenter Server that resides in the AMP-VX management folder.

When hosting VMware vCenter Server environments for existing VxBlock Systems with Dell EMC legacy AMPs on the AMP-VX, consider the following:

- AMP-VX and existing VxBlock System compute hosts must be within the same datacenter and adhere to the 10 ms RTT latency limitations of AMP-VX.
- Any VxBlock System managed by AMP-VX must be at a supported RCM.
- VMware ESXi hosts from a VxBlock System cannot be included in the AMP-VX a VMware vCenter Server cluster and VMware vSAN cluster.

To accommodate hosting the existing VxBlock System VMware vCenter services, a dedicated VMware vCenter Server cluster with VMware Distributed Resource Scheduler (DRS) enabled is created specifically for the existing VxBlock System under the production management folder. The VMs connect to the appropriate VM distributed port group within the VMware vSphere Standard Switch.

The following illustration shows how the VMware vSphere Standard Switch is configured on the AMP-VX:
VMware vSphere Distributed Switch design (VMware vSphere 6.5)

AMP-VX uses DVS-Mgmt with connections to the management switches and DVSwitch-ToR with connections to ToR switches. AMP-VX VMware ESXi host configures VMKernel, VM port groups, and VMware vSAN on the same VMware vSphere Distributed Switch as OOB management.

Both AMP-VX switches use NIOC to prioritize network traffic from VMs. The following table shows NIOC settings for DVSwitch-Mgmt:
<table>
<thead>
<tr>
<th>Traffic type</th>
<th>Shares</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vSAN</td>
<td>High</td>
</tr>
<tr>
<td>NFS</td>
<td>Low</td>
</tr>
<tr>
<td>VMware vSphere vMotion</td>
<td>Low</td>
</tr>
<tr>
<td>VMware vSphere replication</td>
<td>Low</td>
</tr>
<tr>
<td>Management</td>
<td>Normal</td>
</tr>
<tr>
<td>VMware vSphere Data Protection backup</td>
<td>Low</td>
</tr>
<tr>
<td>VM</td>
<td>High</td>
</tr>
<tr>
<td>Fault Tolerance</td>
<td>Low</td>
</tr>
<tr>
<td>iSCSI</td>
<td>Low</td>
</tr>
</tbody>
</table>

The following table shows NIOC settings for DVSwitch-ToR:

<table>
<thead>
<tr>
<th>Traffic type</th>
<th>Shares</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vSAN</td>
<td>Low</td>
</tr>
<tr>
<td>NFS</td>
<td>Low</td>
</tr>
<tr>
<td>VMware vSphere vMotion</td>
<td>Low</td>
</tr>
<tr>
<td>VMware vSphere replication</td>
<td>Low</td>
</tr>
<tr>
<td>Management</td>
<td>Normal</td>
</tr>
<tr>
<td>VMware vSphere Data Protection backup</td>
<td>Low</td>
</tr>
<tr>
<td>VM</td>
<td>High</td>
</tr>
<tr>
<td>Fault Tolerance</td>
<td>Low</td>
</tr>
<tr>
<td>iSCSI</td>
<td>Low</td>
</tr>
</tbody>
</table>

The VMware vCenter Server manages AMP-VX ESXi hosts that reside in the AMP-VX management folder.

When hosting VMware vCenter Server environments for existing VxBlock Systems with Dell EMC legacy AMPs on the AMP-VX, consider the following:

- AMP-VX and existing VxBlock System compute hosts must be within the same data center and adhere to the 10-ms RTT latency limitations of AMP-VX.
- Any AMP-VX managed VxBlock System must be at a supported RCM.
- VMware ESXi hosts from a VxBlock System cannot be in the AMP-VX management VMware vCenter Server.

To host existing VxBlock System VMware vCenter services, a dedicated VMware vCenter Server cluster with VMware Distributed Resource Scheduler (DRS) is created for the existing VxBlock System under the production management folder. The VMs connect to the appropriate VM distributed port group within the VMware vSphere Distributed Virtual Switch.

The following illustration shows how the VMware VDS is configured on the AMP-VX:
VM placement and VLAN assignment (VMware vSphere 6.5)

The default VMware vCenter Server configuration contains the VMware vCenter Server 6.5 with integrated VMware vSphere Update Manager (VUM).

Beginning with VMware vSphere 6.5, Microsoft SQL is not used since VMware vCenter Server and VMware VUM use the bundled postgres database that is embedded within the VMware vCenter Server.

The following figure provides an example of the VM server assignment for AMP-VX servers with the default configuration for VxBlock Systems with Vision Intelligent Operations and standard switches (Embedded PSC):
The following figure provides an example of the VM server assignment for AMP-VX servers with the default configuration for VxBlock Systems with Vision Intelligent Operations and standard switches (External PSC):
**Note:** Actual placement of the management VMs is determined by high availability, DRS, and affinity rules.

The following figure provides an example of the VM server assignment for AMP-VX servers with the default configuration for VxBlock Systems using VxBlock Central (Embedded PSC):

<table>
<thead>
<tr>
<th>AMP-VX Server 1</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AMP-VX</strong></td>
<td><strong>Element Manager</strong></td>
</tr>
<tr>
<td>VMware vCSA</td>
<td>103</td>
</tr>
<tr>
<td><strong>AMP-VX</strong></td>
<td></td>
</tr>
<tr>
<td>VMware PSC 1</td>
<td>205</td>
</tr>
<tr>
<td><strong>ESRS</strong></td>
<td></td>
</tr>
<tr>
<td>Gateway #1</td>
<td>101</td>
</tr>
<tr>
<td><strong>Element Manager</strong></td>
<td>101</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AMP-VX Server 2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AMP-VX</strong></td>
<td><strong>Vision Intelligent Operations Core</strong></td>
</tr>
<tr>
<td>VMware PSC 2</td>
<td>103</td>
</tr>
<tr>
<td><strong>PowerPath EUMS Appliance</strong></td>
<td>103</td>
</tr>
<tr>
<td><strong>VMware vRealize Log Insight</strong></td>
<td>105</td>
</tr>
<tr>
<td><strong>Element Manager</strong></td>
<td>101</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AMP-VX Server 3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Converged System</strong></td>
<td><strong>Element Manager</strong></td>
</tr>
<tr>
<td>VMware vCSA</td>
<td>105</td>
</tr>
<tr>
<td><strong>Vision Intelligent Operations Core</strong></td>
<td>101</td>
</tr>
<tr>
<td><strong>Converged System</strong></td>
<td>105</td>
</tr>
<tr>
<td>AMP-VX PSC 1</td>
<td></td>
</tr>
<tr>
<td><strong>Element Manager</strong></td>
<td>101</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AMP-VX Server 4</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Converged System</strong></td>
<td><strong>Vision Intelligent Operations MSP</strong></td>
</tr>
<tr>
<td>AMP-VX PSC 2</td>
<td>105</td>
</tr>
<tr>
<td><strong>Cisco DCNM</strong></td>
<td>101</td>
</tr>
<tr>
<td><strong>ESRS Gateway #2</strong></td>
<td>101</td>
</tr>
<tr>
<td><strong>Vision Intelligent Operations MSP</strong></td>
<td>105</td>
</tr>
</tbody>
</table>

**VLAN Legend:**
- 101 vcesys_oob_mgmt
- 101 vcesys_esx_build
- 105 vcesys_esx_mgmt
- 205 amx_esc_mgmt
The following figure provides an example of the VM server assignment for AMP-VX servers with the default configuration for VxBlock Systems using VxBlock Central (External PSCs):
See the appropriate *Dell EMC VxBlock System 1000 Architecture Overview* for a description of specific management components of the AMP-VX.
Virtualization (VMware vSphere 6.5)

VMware vSphere is one of the virtualization platforms that provide the foundation for the private cloud. The core VMware vSphere components are the VMware vSphere ESXi and VMware vCenter Server for management.

In the latest update release of vSphere 6.5, VMware vCenter Server with embedded PSC is the default deployment configuration offered. A single Linux appliance provides the vCenter and VMware Single Sign On (SSO) service.

Note: VMware vSphere 6.7 and VMware vSphere 6.5 are the last VMware vSphere releases that support the deployment of external PSCs. Updates to both of these VMware vSphere versions support Enhanced Linked Mode in embedded PSCs, making external PSCs no longer necessary. Upgrading to VMware vSphere 6.7 update 1 or VMware vSphere 6.5 update 2d enables you to migrate external PSCs to embedded PSCs. For more information about changing to embedded PSCs from external PSCs, consult with your account team.

VMware vSphere includes a pair of VMware Platform Services Controller (PSC) Linux appliances to provide the VMware Single Sign On (SSO) service.

The hypervisors are deployed in a cluster configuration. The cluster enables dynamic allocation of resources, such as CPU, memory, and storage.

VMware vSphere ESXi (VMware vSphere 6.x)

VMware vSphere ESXi Enterprise Plus is the system hypervisor.

Cluster configuration

VMware vSphere ESXi hosts and their resources are pooled together into clusters. These clusters contain the CPU, memory, network, and storage resources available for allocation to VMs. VMware vSphere clusters can scale up to a maximum of 64 hosts. Up to 2,000 hosts can be supported in one VMware vCenter Server instance.

Datastores

AMP-VX uses VMware vSAN for its storage which uses VSANFS as the on-disk format. The maximum size per volume is 62 TB. The maximum VMDK file size is 62 TB.

VMware vCenter Server (VMware vSphere 6.5)

The VMware vCenter Server provides a central management point for hypervisors and VMs.

VMware vCenter Server Appliance (vCSA) is leveraged to manage the virtual infrastructure. VMware vSphere Update Manager (VUM) is integrated with the VMware vCSA and assists with host patch management.

There are at least two VMware vCSAs in the AMP: one for AMP local management and one or more to manage VxBlock Systems.

VMware vCSA provides the following functionality:

- Clones of VMs
- Creates of templates
- Migrates VMs though VMware vMotion and VMware Storage vMotion
- Initially configures VMware Distributed Resource Services (DRS) and VMware vSphere high availability (HA) clusters

VMware vCSA provides monitoring and alerting capabilities for hosts and VMs. System administrators can create and apply alarms to all managed objects, including:
• Data center, cluster, and host health, inventory, and performance
• Data store health and capacity
• VM usage, performance, and health
• Virtual network usage and health.

**Authentication**
VMware Single Sign On (SSO) service integrates multiple identity sources including AD, open LDAP, and local accounts for authentication.

**VMware vCenter Server supported features**
Dell EMC supports the following VMware vCenter Server features:

- VMware Single Sign On (SSO) Service
- VMware vSphere Web Client (used with VxBlock Central)
- VMware vSphere High Availability
- VMware vCenter High Availability (optional with VxBlock Central Operations)
- VMware Distributed Resource Scheduler (DRS)
- VMware vSphere Distributed Switch (VDS)
- VMware Fault Tolerance
- VMware vMotion
- VMware Storage vMotion
- VMware Enhanced vMotion Compatibility (EVC)
- VMware Resource Pools (for VMware vSphere Standard Switch)
- VMware Storage Distributed Resource Scheduler (DRS) (capacity only)
- VMware Storage-driven profiles (user-defined only)
- VMware distributed power management (up to 50 percent of VMware vSphere ESXi hosts)
- VMware Syslog Service
- VMware Core Dump Collector

**VxBlock System VMware vCenter Server (VMware vSphere 6.x)**
The VxBlock System VMware vCenter Server manages the VMware vSphere ESXi environment of the VxBlock System. The VxBlock System VMware vCenter Server uses VMware vSphere Distributed Switch (VDS) for virtual networking.

**AMP-VX VMware vCenter Server (VMware vSphere 6.5)**
The local management workload manages the AMP-VX VMware vSphere ESXi environment.

The AMP-VX VMware vCenter Server includes the following components:

- **Virtual Network Switch**: The AMP-VX VMware vCenter Server uses VMware vSphere Standard Switches or VMware vSphere Distributed Switches.
- **Data center**: The default AMP-VX configuration comes with the XMP data center, which supports all workloads from the AMP-VX and VxBlock Systems. This can be named to identify a data center location or provide a unique name to this AMP-VX environment (for example, NYC1-XMP). It is possible to include multiple VMware vSphere ESXi data centers within a single AMP-VX instance with multiple VMware vSphere ESXi clusters.
VMware vSphere Cluster: One VMware vSphere cluster in the VMware vCenter Server accommodates the AMP-VX core, optional workloads, and AMP-VX ECO workloads. A minimum of four servers per cluster is required to provide the performance and resiliency features of VMware vSAN.

Folders: The following folders are assigned to each type of workload to organize the AMP-VX and VxBlock System management applications.

- **AMP-VX_mgmt**: Contains the VMs that support the AMP-VX VMware vCenter Server and jump server. This folder contains a child folder to separate the local element manager VMs (AMP-VX_local) from the VMware vCenter Server environment.

- **Prod_mgmt**: Contains the VMs that support the VMware vCenter Server environment, element manager and Vision Intelligent Operations or VxBlock Central. This folder contains child folders to further separate the VMware vCenter Server environment (XMP_Prod_Central) from the element managers (XMP_Prod_Cmn). XMP_Prod_Central contains a sub-folder for each instance of VxBlock System VMware vCenter Servers:
  - **XMP_Prod01**: Contains the first production shared management VMware vCenter Server VMs.
  - **XMP_Prod02**: Contains an additional production shared management VMware vCenter Server VMs.

- **XMP_Prod_Cmn**: Contains sub-folders to separate element managers common across all VxBlock Systems, including AMP-VX:
  - **XMPcmn01**: Provides the shared managed VMs that support XMP Vision software or VxBlock Central, Element Manager, Secure Remote Services, Cisco DCNM, and PowerPath across all VxBlock Systems. If desired, more than one XMPcmnxx can be configured to separate the management VMs for each VxBlock System. This vAPP is a member of the XMP_Prod_Cmn folder.
  - **Opt_mgmt**: Contains VMs that support the optional components for VxBlock Systems.
  - **Eco_mgmt**: Contains VMs that support the ecosystem workloads for VxBlock Systems.

Management workloads (VMware vSphere 6.x)

The AMP supports core management workload, Dell EMC optional management workload, and ecosystem workloads.

Core management workload (VMware vSphere 6.5)

The core management workload consists of the AMP-VX and VxBlock Systems management VMware vCenter Servers. These servers contain both AMP management and production shared management workloads. The management applications classified as core workloads are required to manage AMP and the VxBlock System.

Workloads are split up into the following folders under the XMP-CORE cluster:

- **AMP-VX_mgmt**: Manages local components for AMP-VX. The AMP-VX management folder contains the local workloads for the VMware vSphere management components that run the AMP-VX.

- **Prod_mgmt**: Contains the central/shared workloads for the VMware vSphere management components and the common components, such as Cisco Element Manager, Secure Remote Services, Cisco DCNM, and PowerPath.

The shared and common workloads are further separated as subfolders of the production shared management folder.

The following table lists the servers that belong in the AMP-VX and production shared management folders:
## Optional management workload

The Dell EMC optional management workload consists of all the optional software components that are not required components of the VxBlock System.

The **Opt_mgmt** folder resides under VMware vSphere Cluster, XMP-CORE.

### Ecosystem management workload (VMware vSphere 6.x)

The ecosystem management workload consists of non-Dell EMC engineered management tools from Cisco, Dell EMC, and VMware, as well as software certified as VxBlock System-ready, such as VMware vRealize Suite, VMware Horizon View, Cisco UCS Director, ViPR, VMware VMTurbo, and BMC Cloud Lifecycle Management.

**Eco_mgmt** is created under the VMware vSphere Cluster, XMP-Core. To segregate this workload from the other workloads, it may be created on a separate AMP-VX.
Manage AMP-VX (VMware vSphere 6.5)

Vision Intelligent Operations or VxBlock Central and VMware vRealize Log Insight software are used to manage AMP-VX.

VxBlock Central

VxBlock Central is available in a Base option, Workflow Automation option, and Advanced Analytics option.

The VxBlock Central dashboard provides system inventory, health monitoring, and RCM compliance management. VxBlock Central also includes the VxBlock Central Shell shell, which provides network configuration and other capabilities necessary to manage an AMP-VX.

VxBlock Central provides the ability to:

- View the health and RCM compliance of multiple VxBlock Systems.
- View charts of key performance indicators (KPI) for one or more components or elements.
- Download software and firmware components to maintain compliance with the current RCM.
- Track real-time information regarding critical faults, errors, and issues affecting VxBlock Systems.
- Configure multisystem AD integration and map AD Groups to VxBlock Central roles.
- Set up compute, storage, networks, and PXE services, manage credentials, and upload ISO images for server installation.
- Monitor VxBlock System analytics and manage capacity through integration with VMware vRealize Operations (vROps).

Dell EMC recommends using VxBlock Central as your primary management interface for AMP-VX.

VMware vRealize Log Insight software

AMP-VX comes with log analytics provided by VMware vRealize Log Insight software.

VMware vRealize Log Insight delivers heterogeneous and highly scalable log management with intuitive, actionable dashboards, sophisticated analytics and broad third-party extensibility, providing deep operational visibility and faster troubleshooting.

VMware vRealize Log Insight is the syslog server for all AMP-VX components, including AMP-VX hosts, AMP-VX VMware vCenter and production VMware vCenter servers. Any VM running on the AMP-VX servers can also use VMware vRealize Log Insight as their syslog server.

VxBlock Central should be used as the SNMP trap collector for AMP-VX and VxBlock Central components.

For more information about VMware vRealize Log Insight, see VMware Docs.

Management software components (VMware vSphere 6.5)

AMP-VX is delivered with specific installed software components dependent on the selected RCM.

The following components are installed as part of the base configuration for the AMP-VX:

- VxBlock Central
- Microsoft Windows Server
- VMware vSphere Enterprise Plus
- VMware vSphere Hypervisor ESXi
- VMware Single Sign On Service (SSO)
- VMware Platform Services Controller (PSC)
Configure system monitoring (VMware vSphere 6.x)

Configure system monitoring for the AMP-VX server using the iDRAC interface.

Before you begin
Verify access to the iDRAC interface.

Procedure

1. Log in to the iDRAC interface of the node.
2. Select Configuration > System Settings > Alerts or Alert: Configuration and confirm Enabled is selected. If not, select Enabled and click Apply.
3. Under Alerts and Remote System Log Configuration, select the alerts to enable and click Apply.
4. Select the SNMP Traps Configuration tab.
   Note: The community string should already be populated for the software server and should not be removed.
5. To add a second destination IP address for an existing monitoring system, type the address into the Alert Destination2 IP field, check State and click Apply.
   Note: Monitoring must support SNMP v2 and use the community string configured on the AMP-VX server for Vision software or VxBlock Central.
6. Under Destination Email Addresses, for each parameter, type the following:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Alert 1-4</td>
<td>email address to send the alert.</td>
</tr>
<tr>
<td>Primary SMTP (email) server IP address or FQDN /DNS Name</td>
<td>IP address associated with the primary SMTP server to which email is sent.</td>
</tr>
<tr>
<td>Enable Authentication</td>
<td>Check this box if the SMTP server requires SMTP authentication. This also enables setting the username and password.</td>
</tr>
<tr>
<td>Username</td>
<td>Type the username which is part of the authentication credentials for the primary SMTP server. Used only if authentication is enforced.</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password which is part of the authentication credentials for the primary SMTP server. Used only if authentication is enforced.</td>
</tr>
</tbody>
</table>
Parameter | Entry
---|---
SMTP port number | If an SMTP port other than 25 is used (for example, 587).

7. Click **Apply**.

### Manage VMware vSphere operations (VMware vSphere 6.5)

Use the VMware vSphere client to perform management tasks on AMP-VX.

You can perform the following management tasks on the AMP-VX:

- Monitor VMware vSAN.
- To manage servers and hosts, see the *VMware vCenter Server and Host Management* in the *VMware vSphere 6.5 Documentation Center*.
- To administer VMware vSphere, see the *VMware vSphere Administration with the vSphere Client* in the *VMware vSphere 6.5 Documentation Center*.

### Related information

- [VMware vSphere 6.5 Documentation Center](#)

### Monitor VMware vSAN (VMware vSphere 6.5)

Monitor VMware vSAN on the AMP-VX.

**About this task**

**Note:** Exercise caution when accessing the AMP-VX VMware vCenter Server. Do not make any configuration changes other than those documented because it may result in loss of monitoring and remote support capabilities.

**Procedure**

1. Launch the VMware vSphere web client and log in.
2. From **Hosts and Clusters**, select the cluster hosting the AMP-VX servers.
3. Select **Manage > Settings > vSAN > General**.
4. To verify the VMware vSAN status, verify the following:
   a. The correct number of flash drives and data disks is displayed.
   b. The network status displays normal.
5. Select **Monitor > vSAN > Health**.
6. Verify all tests pass. If **Warning** or **Failed** is displayed, investigate and troubleshoot the cause.

### Prepare the VMware vSphere ESXi server for temporary maintenance (VMware vSphere 6.5)

When preparing the server for maintenance activities, VMware ESXi hosts using VMware vSAN software-defined storage require specific instructions.

**About this task**

**Note:** Do not use this procedure if the server must be offline for a long period of time or powered off.

**Procedure**

1. Log in to the VMware vCenter Server and select **Hosts and Clusters**.
2. Locate and right-click the VMware vSphere ESXi host, and select **Maintenance Mode > Enter Maintenance Mode**.
3. Verify **Ensure data accessibility from other hosts** is checked.
4. Monitor tasks in **Recent tasks**.
5. Verify the host is in **Maintenance Mode** in the **Navigator** window.

**Prepare the VMware vSphere ESXi server for shutdown (VMware vSphere 6.5)**

When preparing a server shutdown, VMware ESXi hosts using VMware vSAN software-defined storage require specific instructions.

**Procedure**

1. Log in to VMware vCenter Server.
2. From the home window, select **Hosts and Clusters**.
3. Locate and right-click the VMware vSphere ESXi host to shut down, and select **Maintenance Mode > Enter Maintenance Mode**.
   a. Verify **Move powered-off and suspended virtual machines to other hosts in the cluster** is checked.
   b. Select **Evacuate all data to other hosts** and click **OK**.
   c. Monitor tasks in **Recent tasks**.
   d. Validate the host is in **Maintenance Mode** in the **Navigator** window.
4. Right-click the VMware vSphere ESXi host and select **Actions > Power > Shut down**.

**Boot the VMware vSphere ESXi host (VMware vSphere 6.5)**

Boot the VMware vSphere ESXi host from the iDRAC interface.

**Procedure**

1. Log in to the iDRAC interface.
2. Select **Power on System** and click **OK**.
3. Monitor power up from the **Dashboard Virtual Console** window or launch the virtual console.
4. When VMware vSphere ESXi has finished loading, log in to the VMware vCenter Server.
5. Navigate to **Hosts and Clusters**.
6. Validate the host is in **Maintenance Mode** and **not responding does not display**.
   Refresh the VMware vCenter Server window if necessary.
7. Right-click the serviced host and select **Maintenance Mode/Exit Maintenance Mode**.
8. Monitor recent tasks for completion.
9. To validate VMware vSAN health, perform the following steps:
   a. Click the **AMP-VX Cluster** and select **Monitor > vSAN > Health** menu item.
   b. Select **Retest**.
   c. Look for any warnings and run recommended steps.

   **Note:** Procedures that slow or consume excessive resources should be run during maintenance hours only. For example, **Proactive Rebalance Disks** should be run during a maintenance window.

d. If there is a warning on **Cluster - vSAN Disk Balance**, select **Proactive Rebalance Disk**.
e. Navigate to **Host and Clusters**.
f. Select **XMP-Core cluster** (the cluster name may be different).
g. Select the **Configure** tab and select **vSAN/Disk Management**.
h. Select the host from the top window.
i. Verify the following:
   - Five of five disks are in use, connected, and healthy.
   - One disk group is mounted, healthy, and all flash.
   - Five healthy and mounted disks are listed in the bottom window, all flash:
     - One cache disk
     - Four capacity disks

10. Navigate to **Hosts and Clusters** and select a host.
11. Select **Hosts > Configuration > Datastore**.
12. Verify the VMware vSAN datastore device is listed as a datastore on the host.

**After you finish**

For more information, see *Dell EMC Converged System Powering On and Off Guide*.

**Install the latest VMware vSphere ESXi patch (VMware vSphere 6.5)**

After installing the latest patch, when you update a VMware vSphere ESXi host to a newer supported build, the host no longer shares the same build.

**About this task**

Use the VMware vSphere Update Manager (VUM) if upgrading to a newer supported build. You can use the CLI to install the patch. Do not use this procedure for major upgrades.

**Before you begin**

- Verify AMP-VX iDRAC, hosts, VMware vSphere environment and VMware vSAN health check have no warnings or errors. Correct any warnings or errors before proceeding with the upgrade.
- Verify the host is in **Maintenance** mode.
  - Select **Move powered-off and suspended virtual machines to other hosts in the cluster**.
  - Select **Evacuate all data to other hosts** and select **OK**.
- Only a single AMP-VX host can be placed into maintenance mode at a time.
- AMP-VX host software upgrades must be sequential.
- Verify software compatibility for the following:
  - AMP-VX Dell PowerEdge servers BIOS firmware
  - iDRAC firmware
  - HBA330 mini driver firmware
  - Mellanox adapter firmware
  - Intel X550 firmware
  - The build to which you are upgrading

**Note:** You may need to upgrade third-party software prior to updating to the latest release of VMware vSphere ESXi.
- Obtain the **Release Certification Matrix** and **Release Notes** with the version to which you want to update.
Look for the supported version of the VMware patch (build) in the *Virtualization* section.

Determine which patch to install

**Procedure**

1. Download the latest VMware vSphere ESXi patch supported for this release.
2. Using a browser, go to the download center on the *Support* site.
3. Select and download the latest supported VMware vSphere ESXi patch.
4. Install the patch as described in *VMware knowledge base article 2008939*.
5. To verify the installation, on the VMware vSphere ESXi host, confirm the build number matches the update just applied.
6. Reboot the VMware vSphere ESXi host.
7. After the host reboots, remove the host from maintenance mode.
8. Verify AMP-VX iDRAC, hosts, VMware vSphere environment and VMware vSAN health check have no warnings or errors. Correct any warnings or errors before proceeding with upgrades of the remaining AMP-VX hosts.

**Related information**

- **VMware Knowledge Base**
- **Support**

**Patch VMware vSphere ESXi hosts with the VMware vSphere Update Manager (VMware vSphere 6.5)**

When a new VMware vSphere ESXi host is deployed or requires an update, patch VMware vSphere ESXi hosts with the VMware vSphere Update Manager (VUM).

**Before you begin**

- Verify that the patch bundle is listed on the latest version of the *Release Certification Matrix*.
- Verify the software compatibility for the AMP-VX components listed on the RCM. You may need to upgrade third-party software prior to updating to the latest release of VMware vSphere ESXi.
- Verify AMP-VX iDRAC, hosts, VMware vSphere environment, VMware vSAN health check have no warnings or errors.
  - Correct any warnings or errors before proceeding with the upgrade.
  - Only a single AMP-VX host can be placed into maintenance mode at a time.
  - AMP-VX host software upgrades must be sequential.

**Procedure**

1. Log in to VMware vSphere Web Client.
2. Select *Move powered-off and suspended virtual machines to other hosts in the cluster*.
3. Select *Evacuate all data to other hosts* and click *OK*.
   
   **Note:** Do not place more than one AMP-VX host at a time in maintenance mode. AMP-VX VMware VUM host upgrades must be sequential. This allows VMware vCenter Server and the AMP-VX VMware vSAN cluster to continue to operate.

4. In the VMware vSphere Web Client, select the host and select the *Update Manager* tab.
5. Click *Go to Admin View*.
6. From the *Manage* tab, click *Settings* and *Download Settings*.
7. In the *Download Sources* window, select *Import Patches*. 
8. On the Select Patches File page of the Import Patches wizard, browse to the location where you saved the patch or package software bundle, select the file, and click Open.

9. Click Next and wait until the file upload completes successfully.
   If the upload fails, the zip file may have been corrupted during the download process or the incorrect zip file has been imported. Try downloading the zip file again and then import.

10. Click Next.

11. From the Import Patches wizard on the Ready to complete page, verify the package that you imported into the VMware VUM repository and click Finish.

12. Select the Patch Repository tab, and verify the patch appears in the list.

13. Select the Host Baselines tab and click Create to create a new baseline.

14. In the New Baseline wizard:
   a. In the Name and type field, type the package name. For example, HBA330.
   b. For the baseline type, click Host Patch and Next.
   c. In the Patch Options window, leave defaults selected and click Next.
   d. In the Criteria window, select Next.
   e. In the Patches to Exclude window, exclude all patches except HBA330.
   f. In the Additional Patches window, click Next and Finish.

15. Attach the package baseline to the desired VMware vSphere ESXi hosts. You can attach the package baseline to individually selected VMware vSphere ESXi hosts or to multiple hosts by selecting the cluster in the Inventory > Hosts and Clusters.

16. To attach the package baseline to an individual VMware vSphere ESXi host, go to the Compliance view and highlight the desired host in the list to the left of the VMware vSphere Web Client. To attach the package baseline to several VMware vSphere ESXi hosts, perform the following:
   a. In the left-side list, select a folder, cluster, or datacenter.
   b. In the right window, select the Update Manager tab and then click Attach Baseline.
   c. Under Individual Baselines page, select the package baseline that was previously created and click OK.

17. Click Scan for Updates and click OK. Check for the Compliance Status for the attached baseline.

18. Staging is the process of pushing the package onto individual VMware vSphere ESXi hosts from the VMware VUM server. To stage the baseline, perform the following:
   a. In the Update Manager tab, in the Independent Baselines list, highlight the package baseline that was created.
   b. Click Stage Patches.
   c. When the Stage Patches Wizard is displayed, under the Baselines Name column in the Baselines list, verify the package baseline that was created is selected. Do not alter the default Name selection and click Next.
   d. In the Hosts window, all the VMware vSphere ESXi hosts to which the package baseline is attached are selected by default. If required, alter the default Host selection to stage the baseline to only one or some of the VMware vSphere ESXi hosts and click Next.
   e. In the Patch and Extension Exclusion window, verify package information and click Next.
   f. When the Ready to Complete window appears, verify the information and click Finish.

19. During remediation, packages are installed on hosts that do not have the package and/or the package is updated on hosts that have an outdated package. To remediate the baseline, perform the following steps:
   a. Highlight the VMware vSphere ESXi host to remediate and select Update Manager tab.
b. Under **Independent Baselines**, highlight the package baseline that was created and click **Remediate**.

c. From the **Remediate** page, in the **Baseline Groups and Types** section, Extension Baselines is selected by default. In the Baselines list, the package baseline that was created is selected by default. The default **Baseline Groups and Types and Extension Baselines** default selections should not be altered. Click Next.

d. In the **Select target objects** page, all the VMware vSphere ESXi hosts to which the package baseline is staged are selected by default. Alter the default Host selection to remediate the baseline to only the VMware vSphere ESXi host that is in maintenance mode. Click Next.

e. When the **Patches and Extensions** window appears, verify the information and click Next.

f. In the **Advanced options** page, click Next and click Next again.

g. When Ready to Complete window appears, verify the information and click Finish.

20. Once VMware VUM has completed patching the ESXi host, remove the host from maintenance mode.

21. Verify AMP-VX iDRAC, hosts, and VMware vSphere environment have no warnings or errors. Verify VMware vSAN health check does not have any warnings or errors. Correct any warnings or errors before proceeding with any further host upgrades.

22. To proceed with the upgrade of the remaining AMP-VX hosts, perform the following steps:

   a. Select the VMware vSphere ESXi host, right-click and select **Maintenance mode > Enter Maintenance Mode**.

   b. Select **Move powered-off and suspended virtual machines to other hosts in the cluster**.

   c. Select **Evacuate all data to other hosts** and click OK.

      **Note:** With AMP-VX, do not place more than one AMP-VX host at a time in maintenance mode.

   d. Repeat Step 21 for each remaining AMP-VX host to be upgraded.

---

**Manage VMware Single Sign On (VMware vSphere 6.x)**

VMware vCenter Single Sign On (SSO) is an authentication mechanism used to configure security policies and lock out or disable an account for VMware vSphere 6.5. Default policies do not require modification. You may have to modify policies or accounts if regulations require different policies or when troubleshooting a problem.

**Unlock and reset the VMware Single Sign On administrator password (VMware vSphere 6.x)**

The VMware vSphere knowledge base article **KB 2034608** contains instructions to unlock a VMware Single Sign On (SSO) administrator account.

**About this task**

For security purposes, the VMware vCenter administrator account is locked after three failed attempts to log in.

**Procedure**

1. Follow the procedure in the VMware knowledge base article **2034608**.

**Manage the lockout status of VMware vCenter SSO (VMware vSphere 6.7)**

View the lockout status of a VMware vCenter SSO account for VMware vSphere.

**Procedure**

1. Log in to the VMware vSphere Client (HTML5) as an SSO administrator. By default, the user is administrator@vsphere.local.
2. From the home page, select Administration > Single Sign-On > Users and Groups.

3. Each tab shows information from the identity sources about configured accounts that are on the system. Select the Users tab.

4. Select the vSphere.local domain.

5. The Locked or Disabled columns show the status of each configured SSO account. Click the ellipsis vertical bar to Enable/Disable or Unlock.

6. Click Yes to confirm.

Manage the lockout status of VMware Single Sign On (VMware vSphere 6.5)

View the lockout status of a VMware Single Sign On (SSO) account for VMware vSphere.

Procedure

1. Log in to the VMware vSphere Web Client as a VMware SSO administrator. By default, the VMware SSO administrator username is administrator@vsphere.local.

2. From the home page, select Administration > Single Sign-On > Users and Groups.

3. Each tab shows information from the identity sources about configured accounts on the system. Select the Users tab.

4. The Locked or Disabled columns show the status of each configured VMware SSO account. Right-click the appropriate account and select Enable/Disable or Unlock.

   Note: The Locked Users and Disabled Users tabs provide information for the identity sources only.

5. Click Yes to confirm.

Manage VMware vCenter SSO default password policies (VMware vSphere 6.7)

Modify the strict lockout policy of VMware vCenter SSO for VMware vSphere 6.7.

Procedure

1. Log in to the VMware vCenter Client (HTML5) as an SSO administrator. By default, this user is administrator@vsphere.local.

2. From the home page, select Administration > Single Sign-On > Configuration.

3. Select the Policies tab and then select Lockout Policy to view the current lockout policies.

4. To modify the lockout policy, select Edit.

5. Make the required changes and click OK.

Manage VMware Single Sign On default password policies (VMware vSphere 6.0 or 6.5)

Manage the VMware Single Sign On (SSO) default password policies for VMware vSphere.

About this task

By default, the VMware SSO passwords expire after 365 days, including the VMware SSO administrator password. You can modify the expiration policy.

Procedure

1. Log in to the VMware vSphere Web Client as a VMware SSO administrator. By default, this user is administrator@vsphere.local.

2. From the home page, select Administration > Single Sign-On > Configuration.
3. Select the **Policies** tab and click **Password Policies**.

4. To modify the password policy, click **Edit**.

5. Make the required changes and click **OK**.

**Add Windows AD identity source to VMware SSO (VMware vSphere 6.7)**

Associate a Windows AD to the VMware SSO service embedded on the VMware vCenter Server in Embedded PSC Deployments and on separate VMware PSCs for external deployments.

**Before you begin**

Obtain network access to the VMware vCenter Client (HTML5) and use AD domain admin privileges.

**Procedure for Embedded deployments**

1. Log in to the VMware vSphere Client (HTML5) on the element manager VM using the administrator@vsphere.local account at: https://<VCENTER_FQDN OR IP>/ui/

2. Navigate to **Menu > Administration**.

3. Select **Single Sign On > Configuration > Active Directory Domain**.

4. For Embedded PSC deployment, select vCenter server with Embedded PSC and click **Join AD**.

5. Enter the AD domain, username and password (with appropriate AD domain administrative rights).

6. Leave **Organizational unit** blank and click **OK**.

7. Restart the node.

**Procedure for External deployments**

1. Log in to the VMware vSphere Client (HTML5) on the element manager VM using the administrator@vsphere.local account at: https://<VCENTER_FQDN OR IP>/ui/

2. Navigate to **Menu > Administration**.

3. Select **Single Sign On > Configuration > Active Directory Domain**.

4. Perform the following for each PSC:
   - Select the PSC to join to the AD domain and click **JOIN AD**.
   - Leave **Organizational unit** blank and click **OK**.
   - Restart the appliance.

5. Select the **Identity Sources** tab and click **ADD IDENTITY SOURCE** to enter details for the Active Directory domain being added.

6. Select the Active Directory (Integrated Windows Authentication) under **Identity source type**.

7. Verify that the domain name that was previously registered to the PSC is assigned to this AD domain registration.

8. Click **Use machine account > OK**.

9. Select the added AD domain and click **SET AS DEFAULT**.

   While logged in to VMware vCenter Server through the VMware vSphere Client (HTML5) as the administrator@vsphere.local administrative user, assign administrator roles and permissions for domain user accounts or groups that require access to VMware vCenter 6.7.

   By default, only the administrator@vsphere.local account can access VMware vCenter Server until additional permissions are explicitly assigned to domain users.
Add a Windows AD identity source to VMware vCenter SSO (VMware vSphere 6.5)

Associate Windows AD to the VMware vCenter SSO service for VMware vSphere on the VMware PSCs.

About this task
Obtain network access to the VMware vCenter Web Client and AD domain admin privileges.

Procedure
1. Log in to the VMware vSphere Web Client on the Element Manager VM.
   Use the administrator@vsphere.local account and the following URL:
   https://<VCENTER_FQDN OR IP>:9443/vsphere-client/
2. Select Administration > Deployment > System Configuration > Nodes.
3. Select hostname for PSC 2, select the Manage tab and click Settings.
4. Under Advanced, select AD, and click Join…
5. Type the AD domain, username, and password (with appropriate AD domain administrative rights). Leave Organizational unit blank, and click OK.
6. Reboot the PSC Node under the Actions menu.
7. Repeat Steps 2-5 but select the hostname for PSC 1.
8. Reboot the PSC Node under the Actions menu.

   Note: Rebooting the (primary) PSC Node 1 affects the following:
   - All running tasks on the node are cancelled or interrupted.
   - All users currently accessing this node temporarily lose connectivity.
   - If this node is a VMware vCenter Server, features such as DRS and vMotion will temporarily become unavailable.
   - If this node is a PSC, services such as SSO, licensing and certificate, running on this node will temporarily go down.
10. Select the Identity Sources tab, and then click the green + icon to type the details for the AD domain.
11. Select AD (Integrated Windows Authentication) under Identity source type.
12. Verify that the domain name that was previously registered to the PSC is assigned to this AD domain registration.
13. Select Use machine account and click Next.
14. The AD registration is complete. While logged in to VMware vCenter through the Web Client or VMware vSphere Client as the administrator@vsphere.local user, assign Administrator roles/permissions for domain user accounts or groups that require access to VMware vCenter. By default, only the administrator@vsphere.local account can access VMware vCenter until more permissions are explicitly assigned to domain users.
Install VMware vCenter Server root certificates on a web browser (VMware vSphere 6.x)

Install trusted root certificates on Internet Explorer only. For browsers other than Internet Explorer, see browser documentation.

Procedure

1. Open Internet Explorer and go to https://vcsa_fqdn.
2. From the VMware vCenter Server getting started page, select Download trusted root CA certificates and save the file locally.
3. Unzip the downloaded files.
4. Right-click each .crt file and click Open.
5. In the pop up dialog click Install Certificate.

Exact steps may vary depending on the version of the browser. For additional information, see VMware Knowledge Base article 2108294.

Related information
VMware Knowledge Base

Redirect VMware vCenter Server to the secondary external VMware Platform Services Controller (VMware vSphere 6.x)

For VMware vSphere 6.x, repoint the VMware vCenter Server for authentication under the following conditions: the primary external VMware Platform Services Controller (PSC) fails, there are multiple VMware PSCs replicating, and the PSCs are configured without fault tolerance.

Note: VMware vSphere 6.7 and VMware vSphere 6.5 are the last VMware vSphere releases that support the deployment of external PSCs. Updates to both of these VMware vSphere versions support Enhanced Linked Mode in embedded PSCs, making external PSCs no longer necessary. Upgrading to VMware vSphere 6.7 update 1 or VMware vSphere 6.5 update 2d enables you to migrate external PSCs to embedded PSCs. For more information about changing to embedded PSCs from external PSCs, consult with your account team.

See the Repointing the Connections Between vCenter Server and PSC section of the VMware vSphere Installation and Setup Guide.

Related information
VMware docs
Manage multiple VxBlock Systems

A single AMP-VX can manage up to eight VxBlock System 1000 platforms or VxBlock System 340, VxBlock System 350, VxBlock System 540, or VxBlock System 740 that are managed by VxBlock 1000 with AMP-VX. Supported VxBlock Systems must go through the AMP consolidation process.

If you have AMP HBA requirements, you can choose to migrate to eMGMT for array management. AMP-VX does not support HBA connectivity.

If multiple VxBlock Systems are managed by a single AMP-VX, a pair of optional Cisco Nexus Switches as part of the second VxBlock System, can aggregate the out-of-band management network. These switches allow the additional VxBlock Systems to be a part of the VMware vSphere environment located on the AMP-VX. Layer 2 connectivity is used between the AMP-VX and the VxBlock System, and Layer 3 connectivity is used from aggregation switches to the external network.

It is best practice that each server in AMP-VX connects only to the ToR and management switches of a single VxBlock System.

Hypervisor Connectivity

The VMware vCenter Server components for the VxBlock System are part of that system. You can use a single VMware vCenter Server for multiple VxBlock Systems (up to the 2000 server limit) or purchase additional VMware vCenter Server licenses to segregate the workloads for each system.

The minimum AMP-VX configuration of four servers supports up to two VxBlock System VMware vCenter Servers. If more than two servers are needed, add additional AMP-VX servers to support the planned workload and ensure all workloads remain running on N-2 servers.

This following illustration shows the VLANs and network topology layer to manage multiple VxBlock Systems when the optional management aggregation switch pair is present:
AMP-VX Integrated Data Protection

Integrated Data Protection software and hardware are in the base AMP build to allow backups of AMP and to provide a trial backup solution for production data. A licensed Avamar Virtual Edition, Avamar Administrator, and Data Domain system is used for backup of the AMP-VX environment.

Besides Avamar Virtual Edition and Data Domain, some highly customized scripts are included to run application-specific backups for certain AMP-VX core workload VMs. Trial versions of Avamar Virtual Edition and Data Domain Virtual Edition are included to back up 500 GB of production data.

Fully licensed data protection products can be purchased to back up VxBlock System data. These components are installed on AMP-VX as Dell EMC optional workloads and require a minimum of five servers on the AMP-VX. Size the AMP-VX appropriately to support the planned backup resources, and enable all management workloads to remain running on N-2 servers.

The following diagram shows the AMP-VX data protection network topology and VLAN assignments:

The following diagram shows the AMP-VX data protection network topology and VLAN assignments for the VMware VDS:
AMP-VX provides backup data protection for the AMP-VX core management workloads and the management and production VMware vCenter Servers and VMware Platform Services Controllers (PSCs). This preconfigured data protection solution performs daily, full backups of these predefined VMs and retains backups for 14 days.

### Avamar Virtual Edition and Data Domain

AMP-VX contains an instance of Avamar Virtual Edition that is integrated with a physical Data Domain system for protection storage.

Avamar is managed by the Avamar Administrator console installed on the element manager for data protection. The administrator console is pre-configured to perform image backups of the AMP-VX core workload VMs, including both management and production VMware vCenter Server Appliances (vCSAs) and VMware Platform Services Controllers (PSCs). In addition to image backups, the Avamar client is installed on the Windows Server based element manager VMs to execute file-level backups of the VMs.

The following table shows the Avamar backup execution schedule:
<table>
<thead>
<tr>
<th>VM</th>
<th>Backup type</th>
<th>Default execution time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management VMware vCSAs</td>
<td>Image</td>
<td>12:00 AM</td>
</tr>
<tr>
<td>Management VMware PSCs</td>
<td>Image</td>
<td>12:00 AM</td>
</tr>
<tr>
<td>Production VMware vCSAs</td>
<td>Image</td>
<td>01:00 AM</td>
</tr>
<tr>
<td>Production VMware PSCs</td>
<td>Image</td>
<td>01:00 AM</td>
</tr>
<tr>
<td>VxBlock Central or Vision software</td>
<td>Image</td>
<td>02:00 AM</td>
</tr>
<tr>
<td>Element manager for data protection</td>
<td>Image</td>
<td>03:00 AM</td>
</tr>
<tr>
<td>Element manager for storage arrays</td>
<td>Image</td>
<td>03:00 AM</td>
</tr>
<tr>
<td>Cisco DCNM</td>
<td>Image</td>
<td>03:00 AM</td>
</tr>
<tr>
<td>PowerPath Management Appliance</td>
<td>Image</td>
<td>03:00 AM</td>
</tr>
<tr>
<td>VMware vRealize Log Insight</td>
<td>Image</td>
<td>03:00 AM</td>
</tr>
<tr>
<td>Element manager for data protection</td>
<td>File</td>
<td>04:00 AM</td>
</tr>
<tr>
<td>Element manager for storage arrays</td>
<td>File</td>
<td>04:00 AM</td>
</tr>
</tbody>
</table>

**Avamar Virtual Edition and VMware vCenter Server Appliance**

The AMP-VX VMware vCenter Server must be added to Avamar as a VMware vCenter client to perform image backups and restores of VMware VMs. Deployment of an Avamar proxy to the AMP-VX cluster with access to the vSAN datastore is also required to protect VMs within the vSAN datastore.

To add VMware vCenter Server as an Avamar client and to deploy the Avamar proxy, use a VMware vCenter Server user account with the appropriate privileges for authentication. Although the `administrator@vsphere.local` is sufficient, it is best practice to create a user account with only the necessary privileges for this purpose. AMP-VX has a user account (`adp-avadmin@vsphere.local`) created for this reason.

To manage Avamar image backup and recovery through VMware vCenter Server, use the Avamar Plug-in for VMware vSphere Web Client. The plug-in provides a simple interface through the VMware vSphere web client for backup and restoration. When performing any backup or restoration procedures through the Avamar Plug-in for VMware vSphere Web Client, log into the VMware vSphere Web Client using the `adp-avadmin@vsphere.local` user account.

**Avamar checkpoints**

Avamar performs system checkpoints, by default, at the beginning of the regularly scheduled maintenance process. Checkpoints are system-wide backups of Avamar for disaster recovery. By default, these checkpoints are created and stored on the Avamar system which may be helpful in certain situations. In the event of a deleted or corrupted Avamar instance, these checkpoints may not be accessible.

To avoid this situation, Avamar checkpoint backups are directed to the Data Domain system to allow checkpoints to be obtained directly from the Data Domain system.

**Application-specific scripted backups**

Besides Avamar backups, there are customized scripts to perform application-specific backups for certain VMs.

The following VMs have customized scripts:

- VMware vCenter Server Appliance (vCSA)
- VMware Platform Services Controller (PSC)
PowerPath Management Appliance
Backup of the VMware vCenter Server database and VMware vSphere Distributed Switches (VDS)
VMware vRO

These scripts reside on the element manager for data protection which has preconfigured tasks within Microsoft Task Scheduler for execution. The scheduled scripts execute backups through the applications native command-line. Backup file(s) are sent through the command-line to a repository on the element manager for data protection through FTP or SCP.

The backups performed by these scripts require an administrative username and password such as admin, administrator@vsphere.local, or root, as well as the FQDN and display name for the VMs to be backed up. During the factory logical build of the Integrated Data Protection backup solution, an interactive PowerShell script named Configure-Credentials.ps1 was executed to update the CPSD-DP-Settings.cfg file with these inputs.

You can execute the same script to update or add the username, password, FQDN and display name of a protected VM. The script is on the element manager for data protection in D:\DataProtection\BIN.

Execute the script:
- To add another production VMware vCenter Server.
- When you change the administrator@vsphere.local or VMware vCSA root password.
- When you change the root or admin password of the Cisco DCNM or PowerPath Management Appliance instances.
- When you change the FQDN of Cisco DCNM or PowerPath Management Appliance instances.

All passwords entered and stored in the CPSD-DP-Settings.cfg file are stored in an encrypted format. For information on how passwords are encrypted, see Password Security.

Related concepts
Password security on page 82

Password security

Passwords that are typed during CPSD-Configure-Credentials.ps1 script execution are placed into a nonreadable variable as a SecureString.

When the password is typed as a SecureString, the password is encrypted with a 256-bit encryption key. The password is first read from an encryption key file, and written to CPSD-DP-Settings.cfg.

The CPSD-Configure-Credentials.ps1 script checks if the encryption key file is located in D:\DataProtection\PSW on the data protection element manager. The encryption file contains the key that is used for the encryption of the passwords before they are written to CPSD-DP-Settings.cfg. If the encryption file is missing, the script automatically creates an encryption key file.

Change administrator passwords

Change passwords every six months, every quarter, or when key personnel are no longer employed.

When the administrator@vsphere.local password for VMware vCenter or the root password changes for Cisco DCNM or PowerPath Management Appliance, encrypted passwords in CPSD-DP-Settings.cfg must also change. Otherwise, system backups may be interrupted.

Later procedures update the CPSD-DP-Settings.cfg with the new passwords in the encrypted format. It also provides for changing of the hostname/FQDN, and display name for each VM.
Update the CPSD-DP-Settings.cfg file

Update the CPSD-DP-Settings.cfg with new usernames, passwords, FQDNs, and display names for each VM.

About this task

It is best practice for system administrators to change passwords every six months, every quarter or when key personnel are no longer employed.

If you change administrator@vsphere.local password for VMware vCenter or the root password, you must also change the encrypted passwords within the CPSD-DP-Settings.cfg to avoid the interruption system backups.

The following procedures update the CPSD-DP-Settings.cfg with the new passwords in the encrypted format. It also provides for changing of the hostname/FQDN, and display name for each VM.

While proceeding through the script, you do not need to enter information at all prompts. Current information appears at the prompts and may be accepted as is, if no changes required. If the prompt requires new information, type the appropriate information and continue through the script.

Before you begin

For any system requiring updates, obtain the following:

- Display names
- FQDNs
- Usernames
- New passwords

Useful notes when running this script:

- To exit the script, type N at the first prompt.
- From the second prompt on, type N at any prompt to continue to the next prompt.
- At the appropriate prompt, select 2 - AMP-VX
- At the appropriate prompt, select either AMP-VX with External PSCs or AMP-VX without External PSCs

Note: VMware vSphere 6.7 and VMware vSphere 6.5 are the last VMware vSphere releases that support the deployment of external PSCs. Updates to both of these VMware vSphere versions support Enhanced Linked Mode in embedded PSCs, making external PSCs no longer necessary. Upgrading to VMware vSphere 6.7 update 1 or VMware vSphere 6.5 update 2d enables you to migrate external PSCs to embedded PSCs. For more information about changing to embedded PSCs from external PSCs, consult with your account team.

- At the appropriate prompt, select the correct number of production VMware vCenter Server environments to be protected
- Type Y at the Would you like to enter the AMP credentials now? (Y/N) prompt to change the display name, FQDN, username, and/or passwords for the following items:
  - FTP server (element manager for data protection)
  - Management VMware vCenter Server Appliance (vCSA)
  - Management VMware vCenter Server
  - Management VMware Platform Services Controller (PSC)
  - Encryption password for VMware vCSA and VMware PSC backups
  - PowerPath Management Appliance
  - Cisco DCNM appliance
  - VMware vRO
• When Would you like to enter the PROD<1-8> credentials now? (Y/N) is displayed, type Y to change the FQDN, credentials, and passwords for the production Management VMware vCenter Servers, VMware vCSAs and VMware PSCs.

• When Would you like to..? is displayed, type the required information or type N to continue.

• If VMware Enhanced Linked Mode (ELM) is configured, see Perform VMware Platform Services Controller backups in a VMware Enhanced Linked Mode environment before starting.

• Use only the provided script to update the configuration file.

Note: Do not use text editors such as Notepad, WordPad, Notepad++, or Excel to edit CPSD-DP-Settings.cfg.

Procedure

1. From the VMware vSphere Web Client console, log in to the element manager for data protection as local Administrator.

2. Launch PowerShell as administrator and type the following:

   D:
   cd \DataProtection\BIN
   .\CPSD-Configure-Credentials.ps1

3. The script reads CPSD-DP-Settings.cfg, then requests the following input:

<table>
<thead>
<tr>
<th>System</th>
<th>FQDN example</th>
<th>Display name examples</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP</td>
<td>M01EM01.abc.com</td>
<td>M01EM01</td>
<td>Windows server FTP user account: CPSD-DP-FTP</td>
<td>&lt;new_password&gt;</td>
</tr>
<tr>
<td>Management VMware vCSA</td>
<td>M01VCSA01.abc.com</td>
<td>M01VCSA01</td>
<td>Root username: root</td>
<td>&lt;new_password&gt;</td>
</tr>
<tr>
<td>Management VMware vCenter Server</td>
<td>M01VCSA01.abc.com</td>
<td>M01VCSA01</td>
<td>SSO username: <a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
<td>&lt;new_password&gt;</td>
</tr>
<tr>
<td>Management VMware vCSA</td>
<td>M01VCSA01.abc.com</td>
<td>M01VCSA01</td>
<td>No username Backup Encryption Password This password required in the event of a VMware PSC restore.</td>
<td>&lt;new_password&gt;</td>
</tr>
<tr>
<td>Management VMware PSC1/2</td>
<td>M01PSC01.abc.com or M01PSC02.abc.com</td>
<td>M01PSC01 or M01PSC02</td>
<td>Root username: root</td>
<td>&lt;new_password&gt;</td>
</tr>
<tr>
<td>Management VMware PSC1/2</td>
<td>M01PSC01.abc.com or M01PSC02.abc.com</td>
<td>M01PSC01 or M01PSC02</td>
<td>SSO username: <a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
<td>&lt;new_password&gt;</td>
</tr>
<tr>
<td>Management VMware PSC1/2</td>
<td>M01PSC01.abc.com or M01PSC02.abc.com</td>
<td>M01PSC01 or M01PSC02</td>
<td>No username Backup Encryption Password This password required in the event of a VMware PSC restore.</td>
<td>&lt;new_password&gt;</td>
</tr>
<tr>
<td>System</td>
<td>FQDN example</td>
<td>Display name examples</td>
<td>Username</td>
<td>Password</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------</td>
<td>-----------------------</td>
<td>---------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>PowerPath Management Appliance</td>
<td>V01PPMA01.abc.com</td>
<td>V01PPMA01</td>
<td>Root username: root</td>
<td>&lt;new_password&gt;</td>
</tr>
<tr>
<td>Cisco DCNM</td>
<td>V01DCNM01.abc.com</td>
<td>V01DCNM01</td>
<td>Root username: root</td>
<td>&lt;new_password&gt;</td>
</tr>
<tr>
<td>VMware vRO</td>
<td>V01VRO01.abc.com</td>
<td>V01VRO01</td>
<td>Root username: root</td>
<td>&lt;new_password&gt;</td>
</tr>
<tr>
<td>Production 1-8 VMware vRO</td>
<td>V01VCprod01.abc.com</td>
<td>V01VCprod01</td>
<td>Root username: root</td>
<td>&lt;new_password&gt;</td>
</tr>
<tr>
<td>Production 1-8 VMware vCSA</td>
<td>V01VCprod01.abc.com</td>
<td>V01VCprod01</td>
<td>Root username: root</td>
<td>&lt;new_password&gt;</td>
</tr>
<tr>
<td>Production 1-8 VMware vCenter Server</td>
<td>V01VCprod01.abc.com</td>
<td>V01VCprod01</td>
<td>Root username: root</td>
<td>&lt;new_password&gt;</td>
</tr>
<tr>
<td>Production 1-8 VMware vCSA</td>
<td>V01VCprod01.abc.com</td>
<td>V01VCprod01</td>
<td>No username Backup Encryption Password This password required in the event of a VMware PSC restore.</td>
<td>&lt;new_password&gt;</td>
</tr>
<tr>
<td>Production 1-8 VMware PSC1/2</td>
<td>V01PSC01.abc.com or V01PSC02.abc.com</td>
<td>V01PSC01 or V01PSC02</td>
<td>Root username: root</td>
<td>&lt;new_password&gt;</td>
</tr>
<tr>
<td>Production 1-8 VMware PSC1/2</td>
<td>V01PSC01.abc.com or V01PSC02.abc.com</td>
<td>V01PSC01 or V01PSC02</td>
<td>SSO username: <a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
<td>&lt;new_password&gt;</td>
</tr>
<tr>
<td>Production 1-8 VMware PSC1/2</td>
<td>V01PSC01.abc.com or V01PSC02.abc.com</td>
<td>V01PSC01 or V01PSC02</td>
<td>No username Backup Encryption Password This password required in the event of a VMware PSC restore.</td>
<td>&lt;new_password&gt;</td>
</tr>
</tbody>
</table>

Related concepts
Perform VMware Platform Services Controller backups in a VMware Enhanced Linked Mode environment on page 85

Perform VMware PSC backups in a VMware ELM environment

Configure VMware Enhanced Linked Mode (ELM) only on the production VMware vCenter environments. Do not configure VMware ELM on the AMP management VMware vCenter Server.

An AMP contains one virtual environment for the management system, and one or more virtual environments for the production systems. Each virtual environment has a VMware vCenter Server and two VMware Platform Services Controllers (PSCs) when VMware ELM is configured. You can use VMware ELM to manage up to eight production system virtual environments within in a single VMware SSO domain.

To use VMware ELM, linked VMware vCenter Servers must be in the same VMware SSO domain. When VMware ELM is implemented, the number of VMware PSCs is not the same as if VMware ELM was not implemented.

The following diagram shows the virtual environment for the first production environment (without VMware ELM) with a single VMware vCenter Server (VC01) and two VMware PSCs (PSC01 and PSC02):
The backup scripts are configured to back up this environment without any modifications.

The following illustration shows how the virtual environment looks when a second production environment is added and VMware ELM is implemented:
The first production environment (PROD1) consists of a VMware vCenter Server (VC01) and two VMware PSCs (PSC01 and PSC02). The second production environment (PROD2) consists of a VMware vCenter Server (VC02) and only one VMware PSC (PSC03). Because a single VMware SSO domain is used, VMware PSC03 is replicated to PSC01 and PSC02 to maintain high availability.

Run `.\CPSD-Configure-Credentials.ps1` to configure credentials, and type information for PROD1 as follows:

- vCSA is VC01
- PSC1 is PSC01
- PSC2 is PSC03

When typing the information for PROD2, type the information for the VMware vCenter Server and VMware PSC1. VMware PSC1 would be the VM with the name PSC02. When prompted to type the information for PROD2 PSC2, leave the FQDN blank.

The following illustration shows a VMware ELM environment that scales up to eight VMware vCenter Servers and five VMware PSCs:
In a production VMware ELM environment with eight VMware vCenter Servers, backups are configured as follows:

- PROD1
  - VCSA - VC01
  - PSC1 - PSC01
  - PSC2 - PSC05

- PROD2
  - VCSA - VC02
  - PSC1 - PSC02
  - PSC2 - leave empty

- PROD3
  - VCSA - VC03
  - PSC1 - PSC03
  - PSC2 - leave empty

- PROD
  - VCSA - VC04
  - PSC1 - PSC04
  - PSC2 - leave empty
The following rules apply to back up the VMware PSCs:

- **PROD5**: back up the first and the last VMware PSC appliance.
- **PROD6** through **PROD4**: back up the VMware PSC the VMware vCenter Server is pointed at.
- **PROD5** through **PROD8**: do not backup any VMware PSCs. The VMware PSC the VMware vCenter Server is pointed at is already backed up by PROD1 through PROD4.

### Create the scheduled tasks for all backups

Update Microsoft scheduled tasks for backups if: changes are made to the FQDN or display name, or if production VMware vCenter Servers are added or removed during execution `CPSD-Configure-Credentials.ps1`.

**Procedure**

1. Log in to the element manager data protection VM as local Administrator using the console from within the VMware vSphere web client.
2. Launch PowerShell as administrator and type:
   ```powershell
   D:
   cd \DataProtection\BIN
   .\CPSD-Create-Scheduled-Tasks.ps1
   ```
3. To verify that the scheduled tasks were created, right-click **Start > Run**, type `Taskschd.msc` and click **OK**.
4. In the left window, select **Task Scheduler Library**.
   
   Each backup task is scheduled in 5 minute increments. The script checks for the existence of scheduled tasks with the text `CPSD-backup` in the name. If any tasks are found, the script prompts you to proceed. The script deletes the existing `CPSD-backup` tasks and re-creates them with the data from `CPSD-DP-Settings.cfg`.

### Backup types and locations for Avamar and scripted backups

Backup information for management VM workloads is provided.

The following table provides Avamar backup information:
<table>
<thead>
<tr>
<th>Workload VM</th>
<th>Image backup</th>
<th>File backup</th>
<th>Scripted application file backup</th>
<th>Backup location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management VMware vCSA/VMware vCenter Server</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Image backup - Data Domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Scripted backup - element manager for data protection: D:\DataProtection\backup\VCSA</td>
</tr>
<tr>
<td>Management VMware PSCs</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Image backup - Data Domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Scripted backup - element manager for data protection: D:\DataProtection\backup\PSC1 D:\DataProtection\backup\PSC2</td>
</tr>
<tr>
<td>Management VMware vCenter Server database</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Image backup - Data Domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Scripted backup - element manager for data protection: D:\DataProtection\backup\VCSA-DB</td>
</tr>
<tr>
<td>Production VMware vCSA / VMware vCenter Server</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Image backup - Data Domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Scripted backup - element manager for data protection: D:\DataProtection\backup\VCSA</td>
</tr>
<tr>
<td>Production VMware PSCs</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Image backup - Data Domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Scripted backup - element manager for data protection: D:\DataProtection\backup\PSC1 D:\DataProtection\backup\PSC2</td>
</tr>
<tr>
<td>Production VMware vCenter Server databases</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Image backup - Data Domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Scripted backup - element manager for data protection: D:\DataProtection\backup\VCSA-DB</td>
</tr>
<tr>
<td>Production VMware VDS</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Scripted backup - element manager for data protection: D:\DataProtection\backup\VCSA-VDS</td>
</tr>
<tr>
<td>VMware vRealize Log Insight VMs</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Image backup - Data Domain</td>
</tr>
<tr>
<td>Cisco DCNM</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Image backup - Data Domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Scripted backup - element manager for data protection: D:\DataProtection\backup\DCNM</td>
</tr>
<tr>
<td>PowerPath Management Appliance</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Image backup - Data Domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Scripted backup - element manager for data protection: D:\DataProtection\backup\PPMA</td>
</tr>
<tr>
<td>Element manager for data protection</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Image backup - Data Domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>File backup - Data Domain</td>
</tr>
<tr>
<td>Element manager for array management</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Image backup - Data Domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>File backup - Data Domain</td>
</tr>
</tbody>
</table>
### RESTORE FROM BACKUP

Some backup restoration procedures contain a preferred method for restoration and an alternative method.

Methods to restore backups includes image restores, file level restores, and application database restores. Best practice is to follow the preferred method of restoration. Use the alternative method only if the preferred method fails to produce the desired result.

For all restores from Avamar backups, click **Activity** within the Avamar Administrator Console to monitor the progress of the restore.

### RESTORE AN AVAMAR IMAGE USING THE AVAMAR ADMINISTRATOR CONSOLE

AMP-VX management VMs using image backups should always be restored to a new VM.

**Before you begin**

Ensure the original VM has been removed from the VMware vCenter Server Appliance (vCSA) inventory and deleted from disk.

**Procedure**

1. Log in to Avamar Administrator console.
2. Click **Backup and Restore**.
3. From the center window, select the **Restore** tab.
4. Expand the VMware vCSA container and select **Virtual Machines**.
5. Select the VM to be restored.
6. Select the date that contains the backup to be restored.
7. Next to the calendar, select the number associated with the backup.
8. Check **All virtual disks**.
9. From the top menu, select **Actions > Restore now**.
10. Select **Restore to new virtual machine**.
11. Click **Configure Destination**.
12. In the **New Virtual Machine** wizard, type the original name of the VM, select the appropriate folder and click **Next**.
13. Select the appropriate cluster and click **Next and Finish**.
14. Click More Options and ensure the correct Plug-In Type is selected.
15. Ensure Use Changed Block Tracking is selected and click OK.
16. Click OK to start the restore process.

**Restore an Avamar image using VMware vSphere Web Client**

Restore an image of a VM from an Avamar image backup using the VMware vSphere Web Client. AMP-VX management workload VMs should always be restored to a new VM.

**Before you begin**

Ensure the original VM has been removed from the VMware vCenter Server inventory and deleted from disk.

**Procedure**

1. Log in to VMware vSphere Web Client as adp-avadmin@vsphere.local.
2. Select the Home tab and click Backup and Recovery.
3. Select the Restore tab and click the VM to restore.
4. Select the appropriate backup image and click Restore.
5. From Select Backup, click Next.
6. From Set Restore Options, type the name for the VM.
   This is usually the original name of the VM unless another name is desired.
7. Click Choose to select the destination.
   Typically, this is the original location of the VM, unless another location is desired.
8. Under Advanced options, vsanDatastore is pre-selected. Select Power On and reconnect NIC preference.
9. Click Next.
10. At Ready to Complete, click Finish to begin the restore.

**Restore an instant access Avamar image using the VMware vSphere Web Client**

Perform an instant access image restore of a VM from an Avamar image backup using the VMware vSphere Web Client.

**About this task**

Perform this restore if the VM needs to be accessible immediately, or if restoring a VM registered with VMware vCenter Server. This process mounts an NFS share datastore to a VMware vSphere ESXi host and adds the VM to inventory. This restored VM will have the same MAC address and IP address as the original VM.

Once instant access restore has been completed and the original VM has been removed from VMware vCenter Server, storage VMware vMotion may be used to migrate the VM to the VMware vSAN datastore. If the original VM is still registered to VMware vCenter Server, and powered on with the NIC connected, the restored VM should only be powered on with the NIC disconnected.

**Procedure**

1. Log in to VMware vSphere Web Client as adp-avadmin@vsphere.local.
2. From the Home tab, select EMC Backup and Recovery.
3. Select the Restore tab, then select the VM to restore and the appropriate backup image.
4. Click Instant Access.
5. From Select Backup, click Next.
6. From Set Instant Access Options, type the name for the VM.
**Note:** Typically this is the original name of the VM, but only do so if the original VM is not registered to VMware vCenter. Otherwise type a different name.

7. Click **Choose** to select the destination.

   **Note:** This should be the original location of the VM, unless another location is desired.

8. At **Ready to Complete**, click **Finish** to begin the restore.

9. The VM is restored but in a powered down state. Prior to powering on the restored VM, from the VMware vSphere Web Client, right-click the restored VM and select **Edit Settings**.

10. Ensure the Network adapter **Connect at Power On** option is either selected or not selected based on the use case for the restore. If desired, the restored VM may now be migrated with storage VMware vMotion to the VMware vSAN datastore.

11. To delete the VM that was restored using Instant Access, power down the VM, delete from disk, and unmount the NAS datastore from the appropriate VMware vSphere ESXi host.

   **Note:** The NAS datastore may be named something similar to `Avamar-MOD-1513955818632` and is mounted to the VMware vSphere ESXi host which the VM was a guest.

---

## Restore files from a file-level backup using the Avamar Administrator console

Restore individual or multiple files or folders to the original location or an alternate location.

**Procedure**

1. Log in to Avamar Administrator console.
2. Click **Backup and Restore**.
3. Select the **Restore** tab, and then select **clients**.
4. Select the client that contains the file(s) or folder(s) to be restored.
5. Select the date from which the files are to be restored from.
6. Select the backup number from which the files are to be restored from.
7. Expand the file structure and navigate to the files to be restored.
8. Check the box next to the files to be restored.
9. Click **Action** and select **Restore Now**.
10. To restore the files to the original location, leave **Restore Destination Client** as the default. To restore the files to an alternate location, click **Browse**.

   **Note:** The alternate location system must have the Avamar client installed, and be registered to this Avamar system.

11. Under **Restore Destination Choices** select the appropriate destination for the restore and click **OK**.

---

## Restore files from an image backup using the Avamar Administrator console

Perform a file level restore from an Avamar image backup using the Avamar Administrator Console.

**Procedure**

1. Launch and log in to the Avamar Administrator console.
2. Click **Backup and Restore launch**.
3. Select the **Restore** tab.
4. Expand vCenter server client and click Virtual Machines.
5. Select the client that contains the files that you want to restore.
6. Select the date to use when restoring the files.
7. Select the backup number to use when restoring the files.
8. Under Contents of Backup named…, select Browse for Granular Restore.
9. At the Proxy Selection Prompt, click OK.
10. Expand the file structure and locate the files that you want to restore.
11. Check the box next to the files that you want to restore.
12. Click Action and select Restore Now.
   • To restore files to the original location, leave Restore Destination Choices as the default.
   • To restore files to an alternate location, select Restore everything to a different location.
13. Expand the VMware vCenter Server client, click Virtual Machines, and select the VM to restore.
14. At the prompt, type the administrator username and password and click Log on.
15. Under Browse for Folders or Directories, expand the directory or folders to which to restore to and click OK.
   Alternate location must be a client for image backups.
16. Next to Absolute Destination, click Browse.
17. Click More Options, select Restore Access Control List (ACL) if required, and click OK.

**Restore AMP-VX management VMs**

From an image backup, restore the element manager for storage arrays or data protection VM, or from VMware vRealize Log Insight VMs.

**Restore the element manager for storage arrays VM from an Avamar image backup**

Restore the element manager for storage arrays VM from an Avamar image backup.

**Procedure**

1. To perform image restore from latest known good backup of element manager for storage arrays VM, refer to one of the following procedures:
   • Restore from an Avamar image backup using the Avamar Administrator Console
   • Restore from an Avamar image backup using the VMware vSphere Web Client
2. Once the restore is complete, power on the VM, log in and validate functionality.
3. Refer to Re-establish Avamar image backups for restored VMs and perform the procedure.

**Related tasks**

- Restore from an Avamar image backup using the Avamar Administrator Console on page 91
- Restore from an Avamar image backup using the VMware vSphere Web Client on page 92
- Re-establish Avamar image backups for restored VMs on page 110

**Restore the element manager for the data protection VM**

Restore the element manager for data protection VM from an Avamar image backup.

**About this task**

When restoring the element manager for data protection, the Avamar administrator console must be installed on another system. This can be another element manager or a remote system with network access to the Avamar Virtual
Edition instance on the AMP-VX. Alternatively, the VMware vSphere Web Client Avamar plug-in may be used for this restoration.

To install Avamar Administrator, see Installing Avamar Administrator in the Dell EMC Avamar Administration Guide.

**Procedure**

1. To perform image restore from latest known good backup of element manager for storage arrays VM, see one of the following procedures:
   - Restore from an Avamar image backup using the Avamar Administrator Console
   - Restore from an Avamar image backup using the VMware vSphere Web Client

2. Once the restore is complete, power on the VM, log in and validate the following:
   - Launch the Avamar Administrator Console and log in to validate functionality.
   - Manually run the following tasks from the Microsoft Task Scheduler and ensure the backups are successful to verify application backup scripts and Microsoft backup server are functional:

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Backup Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPNSD-backup AMP DCNM</td>
<td>D:\DataProtection\backup\DCNM</td>
</tr>
<tr>
<td>CPNSD-backup AMP PPVE</td>
<td>D:\DataProtection\backup\PPVE</td>
</tr>
<tr>
<td>CPNSD-backup AMP PSC1</td>
<td>D:\DataProtection\backup\PSC1</td>
</tr>
<tr>
<td>CPNSD-backup AMP PSC2</td>
<td>D:\DataProtection\backup\PSC2</td>
</tr>
<tr>
<td>CPNSD-backup AMP VCSA</td>
<td>D:\DataProtection\backup\VCSA</td>
</tr>
<tr>
<td>CPNSD-backup AMP VCSA-DB</td>
<td>D:\DataProtection\backup\VCSA-DB</td>
</tr>
<tr>
<td>CPNSD-backup AMP PROD &lt;x&gt; PSC1</td>
<td>D:\DataProtection\backup\PSC1</td>
</tr>
<tr>
<td>CPNSD-backup AMP PROD &lt;x&gt; PSC2</td>
<td>D:\DataProtection\backup\PSC2</td>
</tr>
<tr>
<td>CPNSD-backup AMP PROD &lt;x&gt; VCSA</td>
<td>D:\DataProtection\backup\VCSA</td>
</tr>
<tr>
<td>CPNSD-backup AMP PROD &lt;x&gt; VCSA-DB</td>
<td>D:\DataProtection\backup\VCSA-DB</td>
</tr>
<tr>
<td>CPNSD-backup AMP VRO</td>
<td>D:\DataProtection\backup\VxBC-vRO</td>
</tr>
</tbody>
</table>

3. See Establish Avamar image backups for restored VMs and perform the procedure.

**Related tasks**

- Restore from an Avamar image backup using the Avamar Administrator Console on page 91
- Restore from an Avamar image backup using the VMware vSphere Web Client on page 92
- Establish Avamar image backups for restored VMs on page 110

**Restore the VMware vRealize Log Insight VMs from an Avamar image backup**

Perform an image restore from the latest known good backup of the VMware vRealize Log Insight master and worker node VMs.

**Before you begin**

See Restore from an Avamar image backup using the Avamar Administrator Console or Restore from an Avamar image backup using the VMware vSphere Web Client.

**Procedure**

1. To perform image restore from the latest known good backup of element manager for storage arrays VM, perform one of the following procedures:
- **Restore from an Avamar image backup using the Avamar Administrator Console**
- **Restore from an Avamar image backup using the VMware vSphere web client**

2. Power on the master node, then the worker node.

3. Ensure each VM is completely up and running before powering on the next VM.

4. To validate VMware vRealize Log Insight, go to: https://<FQDN_of_LogInsight_Master_Node>

5. Select Options and select Administration.

6. Perform the following actions:

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
</table>
| Verify the version of VMware vRealize Log Insight cluster nodes. | a. Under Management, click Cluster.  
    b. In the Nodes table, verify that the version of each node is as expected. |
| Verify the cluster and integrated load balancer status. | a. In the Nodes table, verify that the status for each node is Connected.  
    b. Under Integrated Load balancer, verify the status is Available |
| Verify that the agents on the monitored management nodes are active. | Under Management, click Agent. |
| Verify that the license key is intact. | a. Under Management, click License.  
    b. Verify that the license status in the table is Active. |
| Verify that the VMware vRealize Log Insight integration with management VMware vCSA and Production VMware vCSA is intact. | a. Under Integration, click vSphere.  
    b. Click Test Connection for the management and production VMware vCenter Server. Verify that the Test successful message appears. |
| Verify that the time configuration of VMware vRealize Log insight is intact. | a. Under Configuration, click Time.  
    b. Verify the NTP Servers page contains the correct NTP settings.  
    c. Click Test to verify that the connection is successful, and verify the successful message appears. |
| Verify that the installed content packs are intact. | a. Click Options and select Content Packs.  
    b. Verify the following content packs are under Installed Content Packs:  
    - Cisco - Nexus  
    - Cisco - UCS  
    - Dell - iDRAC  
    - Dell EMC - VMAX  
    - Dell EMC - VNX Unified  
    - General  
    - VMware - vSAN  
    - VMware - vROps 6.x  
    - VMware - vSphere |
### Task
Verify that the dashboards of the content packs are receiving log information.

### Action
In the VMware vRealize Log insight user interface, click **Dashboards**. In the **Navigator**, under **Content Pack Dashboards**, verify the following dashboards appear:

- Cisco - Nexus
- Cisco - UCS
- Dell - iDRAC
- Dell EMC - VMAX
- Dell EMC - VNX Unified
- General
- VMware - VSAN
- VMware - vRops 6.x
- VMware - vSphere

#### Related tasks
- Restore from an Avamar image backup using the Avamar Administrator Console on page 91
- Restore from an Avamar image backup using the VMware vSphere Web Client on page 92
- Establish Avamar image backups for restored VMs on page 110

#### Restore Cisco Data Center Network Manager

When performing a restore of Cisco Data Center Network Manager (DCNM), restore to an operational VM or restore a deleted or corrupted VM.

### Restore to an operational VM

Restore the Cisco DCNM database only if the original VM is fully functional, but a rollback to a previous database state is required.

#### Procedure

1. Log in to the element manager for the data protection VM and do the following:

   The file may be restored using the Avamar Administrator console from the element manager for data protection VM file-level backups.

   a. Go to the `D:\DataProtection\backup\DCNM` directory.

   b. Copy the appropriate `backup.<date-time>.tar.gz` file to the DCNM VM Appliance `/tmp` directory.

   See **Restore files from a file-level backup using the Avamar Administrator console** for information about this type of restoration. For example, open PowerShell and enter the following commands:

   ```
   d:
   cd \DataProtection\BIN
   .\pscp.exe -pw <DCNM_root_password > D:\DataProtection\FTP\DCNM\<DCNM_Display_Name>\backup.<date-time>.tar.gz root@<DCNM_IP_Address>:/tmp
   ```
2. To establish an SSH session to the Cisco DCNM appliance, log in as root and type:
   ```
   cd /tmp
   appmgr restore dcnm backup.<date-time>.tar.gz
   ```

3. Type `y` and press Enter when prompted with `Do you want to continue?`.

4. Type `y` and press Enter when prompted with `PLEASE SHUTDOWN ALL APPLICATIONS BEFORE RESTORING.`.

5. After the restore is complete, to start all services on the Cisco DCNM VM, type:
   ```
   appmgr start dcnm
   ```

Related tasks

**Restore a corrupt or deleted VM**

If the VM has been deleted or corrupted and is not fully functional, restore the corrupt or deleted VM. This includes deploying and configuring a new Cisco DCNM VM, and restoring the database from a known good backup.

**Before you begin**

Ensure the original Cisco DCNM VM has been removed from VMware vCenter Server Appliance (vCSA).

**Procedure**

1. Deploy the Cisco DCNM VM with same configuration, including network and hostname.

2. Log in to the element manager for data protection and copy the appropriate backup.<date-time>.tar.gz file from the `D:\DataProtection\backup\DCNM` directory to the DCNM VM Appliance/tmp directory.

   The file may be restored using the Avamar Administrator console from the element manager for data protection file level backups. Refer to `Restore files from a file-level backup using the Avamar Administrator console`.

   For example, to open PowerShell, type:
   ```
   d:
   cd \DataProtection\BIN
   \pscp.exe
   -pw <DCNM_root_password>
   D:\DataProtection\FTP\DCNM\< DCNM_Display_Name >\backup.<date-time>.tar.gz root@<DCNM_IP_Address>:/tmp
   ```

3. To establish an SSH session to the Cisco DCNM appliance, log in as root and type:
   ```
   cd /tmp
   appmgr restore dcnm backup.<date-time>.tar.gz
   ```

4. Type `y` and press Enter when prompted with `Do you want to continue?`

5. Type `y` press Enter when prompted with `PLEASE SHUTDOWN ALL APPLICATIONS BEFORE RESTORING...`

6. Refer to `Re-establish Avamar image backups for restored VMs` and perform the procedure.

Related tasks

**Restore files from a file-level backup using the Avamar Administrator console** on page 93
Re-establish Avamar image backups for restored VMs on page 110

## Restore PowerPath Virtual Edition License Management Appliance

Restore PowerPath/Virtual Edition (VE) Management Appliance configuration only if the original VM is fully functional, but a rollback to a previous configuration is required.

If the VM is deleted or corrupt and is not fully functional, restore the corrupt or deleted VM.

### Restore to an operational VM

Restore the PowerPath Management Appliance configuration if the original VM is fully functional, but requires a rollback to a previous configuration.

**Procedure**

1. Log in to the element manager for data protection VM.
   
   If necessary, the file may be restored using the Avamar Administrator console from the element manager for data protection file level backups. See *Restoring files from a file-level backup using the Avamar Administrator console* for information about this type of restoration.

2. Copy the appropriate `backup_PPMA<date-time>.zip` file from the `D:\DataProtection\backup\PPMA` directory on the element manager for data protection to the local system from which you are accessing PowerPath Management Appliance.

3. Log in to the PowerPath Management Appliance as `root`.


5. Under `Import Config Zip`, select `Browse`.
   
   - If accessing the PowerPath Management Appliance from the element manager for data protection, go to `D:\DataProtection\backup\PPMA\<PPMA_Display_Name>`.
   - If accessing PowerPath Management Appliance from another system, go to the directory that the .zip file was copied to. Select the appropriate .zip file for the restore and click `Open`.

6. Click `Import` and click `OK` after the `Are you sure to import the file` prompt.
   
   Once complete, the following message opens: *Backup restored successfully*

7. Navigate to `Inventory > vCenter Servers` and select any VMware vCenter Servers that display as `Not Registered`.

8. Click `Register vCenter Plugin`.

### Related tasks

- *Restoring files from a file-level backup using the Avamar Administrator console* on page 93

## Restore a corrupted or deleted VM

To restore a corrupted or deleted VM, deploy and configure a new PPMA VM, and restore the configuration from a known good backup.

**Procedure**

1. Deploy PPMA VM with same configuration, including networking and hostname.

2. Log in to the element manager for data protection.
   
   a. Go to the `D:\DataProtection\backup\PPMA` directory on the element manager for data protection.
b. Copy the appropriate `backup_PPMA-<date-time>.zip` file to the local system from which you are accessing PowerPath Management Appliance.

If necessary, the file may be restored using the Avamar Administrator console from the element manager for data protection file-level backups. See *Restore files from a file-level backup using the Avamar Administrator console*.

3. Log in to the PowerPath Management Appliance as `root`.


5. Under `Import Config Zip`, select `Browse`. If accessing PowerPath Management Appliance from the element manager for data protection, go to `D:\DataProtection\backup\PPMA`. If accessing PowerPath Management Appliance from another system, go to the directory that the `.zip` file was copied to. Select the appropriate `.zip` file for the restore and click `Open`.

6. Click `Import` and click `OK` on the `Are you sure to import the file` prompt.

   When complete, the following message opens: `Backup restored successfully and providing details of the import`.

7. Navigate to `Inventory > vCenter Servers` and select any VMware vCenter Servers with a status of `Not Registered`.

8. Click `Register vCenter Plugin`.

9. See *Enable scripted backup configuration of the PPMA or VMware vCenter Server Appliances* and perform the procedure.

10. See *Re-establish Avamar image backups for restored VMs* and perform the procedure.

**Related tasks**

- Enable scripted backup configuration of the PPVE or VMware vCenter Server Appliances on page 111
- Restore files from a file-level backup using the Avamar Administrator console on page 93
- Re-establishing Avamar image backups for restored VMs on page 110

### Restore VxBlock Central

Perform a restore of VxBlock Central when the VxBlock Central VMs are corrupt or deleted.

**About this task**

VxBlock Central contains the following VMs:

- Core
- MSM
- MSP
- VxBlock Central Orchestration Services
- VMware vRO

For more restoration procedures for the VxBlock Central, see the *Dell EMC VxBlock System 1000 Administration Guide*.

**Procedure**

1. To restore an image of all VxBlock Central VMs from latest known good backup, see *Restore from an Avamar image backup using the Avamar Administrator Console* or *Restore from an Avamar image backup using the VMware vSphere Web Client*.

2. Using VMware vSphere Web Client, power on the Core VM.

3. Open the Core VM console and monitor the boot process.

4. Once the Login prompt is displayed, use the VMware vSphere Web Client to power on the MSM VM.
5. Open the MSM VM console and monitor the boot process.
6. Once the Login prompt is displayed, using the VMware vSphere Web Client, power on the MSP VM.
7. Open the MSP VM console and monitor the boot process.
8. After the Login prompt is displayed, see Establish Avamar Image backups for Restored VM to perform the procedure.

**Related tasks**
- Restore from an Avamar image backup using the Avamar Administrator Console on page 91
- Restore from an Avamar image backup using the VMware vSphere Web Client on page 92
- Establish Avamar image backups for restored VMs on page 110

## Restore Vision software

Restore Vision software when the Vision software VMs are corrupt or deleted.

**About this task**
For additional restoration procedures for the Vision software environment, review Backup and Restoring from the Dell EMC Vision Intelligent Operations Administration Guide.

**Procedure**

1. To restore an image of all Vision software VMs from latest known good backup, refer to Restore from an Avamar image backup using the Avamar Administrator Console or Restore from an Avamar image backup using the VMware vSphere Web Client.
2. Using VMware vSphere Web Client, power on the Vision software Core VM.
3. Open the Vision software Core VM console and monitor the boot process.
4. Once the Login prompt appears, using the VMware vSphere Web Client, power on the Vision software MSM VM.
5. Open the Vision software MSM VM console and monitor the boot process.
6. Once the Login prompt appears, using the VMware vSphere Web Client, power on the Vision software MSP VM.
7. Open the Vision software MSP VM console and monitor the boot process.
8. After the Login prompt appears, refer to Re-establish Avamar Image backups for Restored VM to perform the procedure.

**Related tasks**
- Restore from an Avamar image backup using the Avamar Administrator Console on page 91
- Restore from an Avamar image backup using the VMware vSphere Web Client on page 92
- Re-establish Avamar image backups for restored VMs on page 110

## Restore VMware vCenter Server Appliance and VMware Platform Services Controllers

Avamar Virtual Edition is configured to perform image backups of the VMware vCenter Server Appliances (vCSAs) and VMware Platform Services Controllers (PSCs) for management and production.

Although Avamar image backups are available for restore and procedures are provided in this guide, the preferred method is to use restore procedures for the scripted backups. Restore the VMware vCSA and VMware PSCs using the Avamar image backups only if the desired result is not obtained through a restore from the VMware vCSA and VMware PSC scripted backups.

The following steps are based on these specific use cases:

- If one VMware PSC is deleted or corrupted, perform the following:
- Repoint the VMware vCenter Server to a remaining functional VMware PSC.
- Rebuild the deleted or corrupted VMware PSC according to VMware procedures for adding a VMware PSC.
- If all VMware PSCs are deleted or corrupted, perform the following:
  - Restore the primary VMware PSC using *Restore a VMware Platform Services Controller using a scripted VMware vCenter backup*.
  - Rebuild all remaining deleted or corrupted VMware PSCs according to VMware procedures for adding a VMware PSC.
  - If VMware vCSA is deleted or corrupted, restore the VMware vCSA using *Restore a VMware vSphere Server Appliance using scripted VMware vCenter backup*.
  - If VMware vCSA and all VMware PSCs are deleted or corrupted, perform the following:
    - Restore the primary VMware PSC using *Restore a VMware Platform Services Controller using a scripted VMware vCenter backup*.
    - Restore the VMware vCSA using the *Restore a VMware vSphere Server Appliance using a scripted VMware vCenter backup*.
    - Rebuild all remaining deleted or corrupted VMware PSCs according to VMware procedures for adding a VMware PSC.
  - If the VMware vCenter Server database needs to be restored to a previously known good state, restore the database using the *Restore the VMware vCenter Server database*.
  - If VMware vSphere Distributed Switch (VDS) is deleted, restore the VMware VDS using the *Import a VMware VDS using VMware VDS export files*.
  - If VMware VDS needs to be restored to a previously known good state, restore the VMware VDS using the *Restore the configuration and settings to an existing VMware VDS using VMware VDS export files*.

**Related tasks**

- *Restore a VMware Platform Services Controller using a scripted VMware vCenter Server Appliance backup* on page 103
- *Restore a VMware vCenter Server Appliance using a scripted VMware vCenter Server Appliance backup* on page 105
- *Restore the VMware vCenter Server database* on page 107
- *Import a VMware VDS using VMware VDS export files* on page 110
- *Restore the configuration and settings to an existing VMware VDS using VMware VDS export files* on page 109

**Deploy replacement VMware Platform Services Controller**

Deploy replacement VMware PSCs before you deploy replacement VMware Platform Services Controllers (PSCs) to join an existing VMware Single Sign On (SSO) site after a VMware PSC is restored.

**Procedure**

1. Log in to the restored VMware PSC as root, and type:

   ```shell
cd /usr/lib/vmware-vmdir/bin
vdcleavefed-h <PSC_FQDN> - u Administrator
```

   Where `<PSC_FQDN>` is the FQDN of the VMware PSC you are attempting to redeploy.

2. To deploy the replacement VMware PSC, refer to the VMware Procedures for adding a VMware PSC.

**Related information**

- VMware docs
Restoring a VMware Platform Services Controller through a scripted VMware vCenter Server Appliance backup

Perform this procedure as the preferred method to restore a VMware Platform Services Controller (PSC) that has been deleted or corrupted, or if a full restore is required of both VMware PSCs and the VMware vCenter Server Appliance (vCSA).

**Before you begin**

Obtain:

- VMware PSC hostname
- Network settings: IP address, subnet mask, default gateway
- IP addresses of DNS servers
- Appropriate entries for name resolution for the VMware PSCs exist in DNS
- Password for VMware vSphere ESXi root account or VMware vCSA administrator account
- FTP user account name
- Backup encryption password

**Procedure**

1. Mount the `VMware-VCSA-all-6.5.x-xxxxxxx.iso`.
2. Navigate to the mounted ISO `vcsa-ui-installer\win32`.
3. Double-click `installer.exe`.
4. From the Installer console, click Restore.
5. From the Restore - Stage 1: Deploy appliance, perform the following actions for each numbered step on the left of the window:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Introduction</td>
<td>Click Next.</td>
</tr>
<tr>
<td>2. End user license agreement</td>
<td>Select I accept the terms of the license agreement and click Next.</td>
</tr>
</tbody>
</table>
| 3. Enter backup details | For Protocol, type: FTP  
For Location, type: `<FTP_SERVER_FQDN >/<FTP_PATH>`  
Example: `m01em01.abc.com/PSC1/<PSC1_Name>/backup--<PSC1_Name>--PSC1-<Date_Time_of_Backup>`  
For Port, type: 21  
For User Name, type: `<FTP_User_Account_Name>`  
Example: `CPSD-DP-FTP`  
For Password, type: `<password_for FTP_user_account_name>` |
| 4. Review backup information | Review and click Next. |
| 5. Appliance deployment target | To restore the management VMware PSC, type: `<FQDN_of VMware_vSphere_ESXi_host>`  
To restore production VMware PSC, type: `<FQDN_of management_vCenter_server>` |
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Backup Details</td>
<td>Type: &lt;encryption_password&gt;</td>
</tr>
<tr>
<td>2. Ready to complete</td>
<td>Review settings and click Finish. Click OK to warning stating once started, restore cannot be paused or stopped.</td>
</tr>
</tbody>
</table>

**Close**

**WARNING:** Please perform the following operations on the management node(s) pointing to this PSC node

8. When **Platform Services Controller 6.5 Restore Complete** appears, click **Close**.
9. Refer to **Re-establishing Avamar Image backups for restored VM** to perform the procedure.
Related tasks
Re-establishing Avamar Image backups for restored VM on page 110

Restore a VMware vCenter Server Appliance through a scripted VMware vCenter Server Appliance backup

This is the preferred method to restore a VMware vCenter Server Appliance (vCSA) if it deleted or corrupt, or if a full restore is required of both the VMware Platform Services Controllers (PSCs) and VMware vCSA.

Before you begin

Obtain:
- VMware vCSA hostname
- Network IP address, subnet mask, default gateway
- DNS server IP addresses
- Entries for name resolution for the VMware vCSA and VMware PSCs that exist in DNS
- VMware vSphere ESXi root account or VMware vCSA root account password
- FTP user account name
- Backup encryption password

Procedure

1. Mount the VMware-VCSA-all-6.5.x-xxxxxxx.iso.
2. Navigate to the mounted ISO vcsa-ui-installer\win32.
3. Double-click installer.exe.
4. From the Installer console, click Restore.
5. From the Restore - Stage 1: Deploy appliance, perform the following actions:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Introduction</td>
<td>Click Next.</td>
</tr>
<tr>
<td>2. End user license agreement</td>
<td>Select I accept the terms of the license agreement and click Next.</td>
</tr>
<tr>
<td>3. Enter backup details</td>
<td>For Protocol, type: FTP</td>
</tr>
<tr>
<td></td>
<td>For Location, type: &lt;FTP_SERVER_FQDN&gt;/&lt;FTP_PATH&gt;</td>
</tr>
<tr>
<td></td>
<td>Example: m01em01.abc.com/VCSA/&lt;VCSA_Name&gt;/backup-&lt;VCSA_Name&gt;VCSA&lt;Date_Time_of_Backup&gt;</td>
</tr>
<tr>
<td></td>
<td>For Port, type: 21</td>
</tr>
<tr>
<td></td>
<td>For User Name, type: &lt;FTP_User_Account_Name&gt;</td>
</tr>
<tr>
<td></td>
<td>Example: CPSD-DP-FTP</td>
</tr>
<tr>
<td></td>
<td>For Password, type: &lt;password_for FTP_user_account_name&gt;</td>
</tr>
<tr>
<td>4. Review backup information</td>
<td>Review and click Next.</td>
</tr>
<tr>
<td>5. Appliance deployment target</td>
<td>To restore the management VMware vCSA, type: &lt;FQDN_of VMware_vSphere_ESXi_host&gt;</td>
</tr>
<tr>
<td></td>
<td>To restore the production vCSA, type: &lt;FQDN_of management_vCenter_server&gt;</td>
</tr>
</tbody>
</table>
### AMP-VX Integrated Data Protection

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Backup Details</td>
<td>Type: &lt;encryption_password&gt;</td>
</tr>
<tr>
<td>2. Ready to complete</td>
<td>Review settings and click Finish. Click OK to warning stating once started, restore cannot be paused or stopped.</td>
</tr>
</tbody>
</table>

### Related tasks
- **Re-establish Avamar Image backups for restored VM on page 110**
- **Enable the scripted backup configuration of the PowerPath/VE or VMware vCenter Server Appliances on page 111**

---

6. **Click Continue** after a message is displayed confirming successful deployment.

7. For **Restore - Stage 2: Deploy Platform Services Controller Appliance**, perform the following:

8. **Click Close** after a message is displayed indicating the restore is complete.

9. Refer to **Re-establish Avamar Image backups for restored VM** to perform the procedure.

10. Refer to **Enable the scripted backup configuration of the PPVE or VMware vCenter Server Appliances** to perform the procedure.
Restore the VMware vCenter Server Appliance database

Perform a restore to a previous state of the VMware vCenter Server database when VMware vCenter Server is in a functional state.

Procedure

1. Establish an SSH session with VMware vCenter Server Appliance (vCSA) and log in as root.
2. To enable shell, type: `shell`
3. To enable VMware vCenter secure copy (SCP) access, type: `chsh -s /bin/bash root`
4. To copy the database backup file from the element manager for data protection to the VMware vCSA, type:

   ```bash
   pscp.exe -pw <vCenter_root_password>
   D:\DataProtection\backup\VCSA-DB\<vCenter_Display_Name>\backup--<vCenter_Display_Name>--VCSA-DB--<Date_Time_of_Backup>.bak root@<vCenter_FQDN>:/backup
   ```

5. To ensure `restore_lin.py` is executable, from the VMware vCSA SSH session, type:

   ```bash
   chmod 700 /backup/restore_lin.py
   ```

6. To stop the `vmware-vpxd` and `vmware-vdcs` services, from the VMware vCSA SSH session, type:

   ```bash
   service-control --stop vmware-vpxd
   service-control --stop vmware-content-library
   ```

7. From the VMware vCSA SSH session run the `restore_lin.py` python script and provide the location for the backup file. For example, type:

   ```bash
   python /backup/restore_lin.py -f /backup/backup-dp--vcenter_display_name--VCSA-DB--<date_time>.bak
   ```

   When the restore completes, a message indicating the restore completed successfully appears.

8. To start the `vmware-vpxd` and `vmware-vdcs` services, from the VMware vCSA SSH session, type:

   ```bash
   service-control --start vmware-vpxd
   service-control --start vmware-content-library
   ```

9. To disable SCP access, from the VMware vCSA SSH session, type:

   ```bash
   chsh -s /bin/appliancesh root
   ```

10. To remove the backup file, type:

    ```bash
    cd /backup
    rm backup-dp--vcenter_display_name--VCSA-DB--<date_time>.bak
    ```
Restore VMware Platform Services Controllers and VMware vCenter Server Appliance using an image backup

Restore from an Avamar image backup of the VMware Platform Services Controller (PSC) and the VMware vCenter Server Appliance (vSCA). This procedure should only be followed if restoring from the VMware vCSA and/or VMware PSC scripted file backups does not produce the desired result.

**About this task**

⚠️ **CAUTION** Perform this procedure as a last resort as it may produce mixed results.

Do not use this procedure to restore only VMware PSCs. It should only be performed when both a VMware PSC and a VMware vCSA is restored. It is preferred to restore VMware PSCs and VMware vCSAs through the scripted backups.

**Procedure**

1. Restore an image of VMware PSC1 and VMware vCSA using Avamar Administrator Console or Avamar Plug-In for vSphere Web Client.
   
   **Note:** In the Restore Command Line Options of the Avamar Restore, **Do not power on VM after restore** should be selected.

2. Power on the VMware PSC VM.

3. Once the VMware PSC VM is powered on, to verify VMware PSC services from the VMware vSphere Web Client console or VMware ESXi web console, log in as **root** and type:

   ```
   service-control --status --all
   ```

   Output similar to the following appears:

   ```
   Running:

   applmgmt lwsmd pschealth vmafdd vmdad vmdird vmdnsd vmonapi vmware-cis-license vmware-cm vmware-psc-client vmware-rhtpproxy vmware-sca vmware-statsmonitor vmware-sts-idmd vmware-stsd vmware-vapi-endpoint vmware-vmon
   ```

   a. If a service is displayed under **StartPending**, wait a few minutes and type:

   ```
   service-control --status --all
   ```

   b. If a service appears under **Stopped**, to start the service, type:

   ```
   service-control --start <service_name>
   ```

4. Power on the VMware vCSA VM.

5. To verify the VMware vCSA service from the VMware vSphere Web Client or VMware ESXi web console, log in as **root** and type:

   ```
   service-control --status --all
   ```
a. If output similar to the following appears:

```
Running:
lwsmd vmafdd
Stopped:
```

Run the `vcenter-restore` script. To do this, type:

```
vcenter-restore -u administrator@vsphere.local -p <administrator@vsphere.local_password>
```

b. When the script completes, type:

```
service-control --status
```

Output should be similar to the following:

```
Running:
Stopped:
vmcam vmware-mbcs vmware-vcha
```

6. Perform **Re-establish Avamar image backups for restored VMs**.

**Related tasks**

Re-establish Avamar image backups for restored VMs on page 110

---

**Restore the configuration and settings to an existing VMware vSphere Distributed Switch**

Restore the configuration and settings to an existing VMware vSphere Distributed Switch (VDS) if a VMware VDS configuration or settings have been changed.

**Procedure**

1. Log in to VMware vSphere Web Client as `administrator@vsphere.local`.
2. From the **Home** tab, select **Networking**.
3. Right-click the VMware VDS to which to restore the configuration.
4. Select Settings > Restore Configuration.
5. Browse to the VMware VDS configuration export found on the element manager for data protection at 
   D:\DataProtection\backup\VCSA-VDS\<vCenter_Display_Name>\backup--
   vCenter_Display_Name>-VCSA--<Date_Time_of_Backup>-vDS

6. Select Restore, then select Restore distributed switch and all port groups or Restore distributed switch only.

7. Click Next and Finish.

**Import a VMware vSphere Distributed Switch**

Import a VMware vSphere Distributed Switch (VDS) using the VMware VDS export file if a VMware VDS is corrupted or unintentionally deleted.

**Before you begin**

Ensure the original VMware VDS has been removed from VMware vCenter Server Appliance (vCSA).

**Procedure**

1. Log in to VMware vSphere Web Client as administrator@vsphere.local.
2. From the Home tab, select Networking.
3. Right-click the VMware vCSA data center to which to import the VMware VDS.
4. Select Distributed Switch > Import Distributed Switch.
5. Browse to the VMware VDS configuration export found on the Element Manager for Data Protection at 
   D:\DataProtection\backup\VCSA-VDS\<vCenter_Display_Name>\backup--
   vCenter_Display_Name>-VCSA--<Date_Time_of_Backup>-vDS

6. Select Preserve original distributed switch and port group identifiers.
7. Click Next and Finish.

**Establish Avamar image backups for restored VMs**

Establish the Avamar Image backups of restored VMs.

**Procedure**

1. From the Avamar administrator console, select Administration launch.
2. Select vCenter > VirtualMachines.
3. Right-click the restored VM name and select Retire Client with the default settings.
4. Navigate to vCenter > Virtual Machines.
5. Right-click New Client.
6. Select the Hosts and Clusters tab and navigate to the AMP-VX cluster.
7. Select the restored VM, ensure Enable Changed Block Tracking is selected and click OK.
8. From the Avamar administrator console, click Policy.
9. Select vCenter > Virtual Machines.
10. In the right window, click the appropriate group based on the following table and click Edit.

<table>
<thead>
<tr>
<th>VM</th>
<th>Group Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Element manager for storage arrays</td>
<td>Core Workload Image Backups</td>
</tr>
<tr>
<td>VM</td>
<td>Group Policy</td>
</tr>
<tr>
<td>-------------------------------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Element manager for data protection</td>
<td>Core Workload Image Backups</td>
</tr>
<tr>
<td>Cisco DCNM</td>
<td>Core Workload Image Backups</td>
</tr>
<tr>
<td>VMware vRealize Log Insight</td>
<td>Core Workload Image Backups</td>
</tr>
<tr>
<td>PowerPath VE Management Appliance</td>
<td>Core Workload Image Backups</td>
</tr>
<tr>
<td>Vision software or Core, MSM, MSP (for VxBlock Central)</td>
<td>Core Workload Image Backups</td>
</tr>
<tr>
<td>Management VMware vCSA</td>
<td>Management VMware vCSA Image Backups</td>
</tr>
<tr>
<td>Management PSCs</td>
<td>Management VMware vCSA Image Backups</td>
</tr>
<tr>
<td>Production VMware vCSA</td>
<td>Production VMware vCSA Image Backups</td>
</tr>
<tr>
<td>Production PSCs</td>
<td>Production VMware vCSA Image Backups</td>
</tr>
</tbody>
</table>

11. In the **Edit Group** console, select the **Members** tab.
12. Locate and select the restored VM and click **Include** and **OK**.

### Enable the scripted backup configuration of the PowerPath/VE appliance or VMware vCenter Server Appliances

Use this procedure to enable backups of the management PowerPath/VE (PPVE) appliance or any of the VMware vCenter Server Appliances (vCSA).

**About this task**

After updating the settings file, run the `.\CPSD-Create-Scheduled-Tasks.ps1` script. This script creates scheduled tasks for the backups and creates scheduled tasks to configure the PPVE and VMware vCSA appliances for backups.

**Procedure**

1. Log in to the data protection element manager VM, as `local Administrator` using the console within the VMware vSphere Web Client.
2. Right-click the **Start > Run**, type `taskschd.msc` and click **OK**.
3. Click **Task Scheduler Library**.
4. Scroll down the list of scheduled tasks in the middle pane and locate tasks that start with **CPSD-Reconfigure**.
5. From the list of **CPSD-Reconfigure** tasks, location the correct application (PPVE or VMware vCSA) and environment (AMP or PROD1 through PROD8). For example, if a restore was done of the first production VMware vCSA, select the scheduled task **CPSD-Reconfigure-PROD1 VCSA-DB**.
6. Right-click the scheduled task and click **Run**.
7. When the task finishes, in the **Last Run Results** column, the following message should open: **The operation completed successfully (0x0)**

If this message does not open, verify the following:

- The appliance is powered up and has finished booting.
- The appliance is reachable by the ping command when using the FQDN. If the FQDN has changed, see *Updating the CPSD-DP-Settings.cfg file with new usernames, passwords, FQDNs, and display names to run the configure credentials script.*
The username and password is the same as they were before the restore. If the credentials were changed, see Updating the CPSD-DP-Settings.cfg file with new usernames, passwords, FQDNs, and display names to run the configure credentials script.

8. Once the restored appliance has been reconfigured, scheduled backups resume.

Related tasks
Updating the CPSD-DP-Settings.cfg file with new usernames, passwords, FQDNs, and display names on page 83

**Restore Avamar Virtual Edition**

If Avamar Virtual Edition is corrupted or the VM is deleted, Avamar Virtual Edition requires a restoration of Avamar from a checkpoint backup.

An Avamar checkpoint is a system-wide backup taken for disaster recovery. Checkpoints occur during the Avamar maintenance, and may also be performed manually as described in the *Dell EMC Avamar Administrator Guide*.

This Avamar Virtual Edition instance has been pre-configured to store the Avamar checkpoint backups on the Data Domain system included with the AMP-VX. Without an Avamar checkpoint backup on the Data Domain, it may not be possible to recover the Avamar instance or access any Avamar backups residing on the Data Domain.

⚠️ **CAUTION** Recovery of an Avamar checkpoint should always be completed with the assistance or engagement of Avamar Technical Support or Professional Services.
**Additional references**

References to related documentation for virtualization, compute, and storage components are provided.

**Compute components**

Compute component information and links to documentation are provided.

<table>
<thead>
<tr>
<th>Product</th>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
</table>

**Virtualization components**

Virtualization component information and links to documentation are provided.

<table>
<thead>
<tr>
<th>Product</th>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vCenter Server</td>
<td>Provides a scalable and extensible platform that forms the foundation for virtualization management.</td>
<td><a href="https://www.vmware.com/products/vcenter-server.html">https://www.vmware.com/products/vcenter-server.html</a></td>
</tr>
<tr>
<td>VMware vSphere ESXi</td>
<td>Virtualizes all application servers and provides VMware High Availability (HA) and Dynamic Resource Scheduling (DRS). (This is available if VMware vSphere Enterprise Plus is licensed on all ESXi hosts inside a cluster.)</td>
<td><a href="http://www.vmware.com/products/vsphere/">www.vmware.com/products/vsphere/</a></td>
</tr>
<tr>
<td>VMware Single Sign On (SSO) Service</td>
<td>Provides VMware-specific authentication services.</td>
<td>blogs.vmware.com/kb/2012/10/vsphere-sso-resources.html</td>
</tr>
<tr>
<td>VMware vSAN</td>
<td>Provides software defined storage networking from VMware.</td>
<td><a href="https://www.vmware.com/products/vsan.html">https://www.vmware.com/products/vsan.html</a></td>
</tr>
</tbody>
</table>

**Network components**

Network component information and links to documentation are provided.

<table>
<thead>
<tr>
<th>Product</th>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vSphere Distributed Switch</td>
<td>Provides centralized management and monitoring of the networking configuration of all hosts that are associated with the switch. A distributed switch is created on a VMware vCenter Server system and its settings are propagated to all hosts associated with the switch.</td>
<td><a href="https://docs.vmware.com/en/VMware-vSphere/6.5/vsphere-esxi-vcenter-server-65-networking-guide.pdf">https://docs.vmware.com/en/VMware-vSphere/6.5/vsphere-esxi-vcenter-server-65-networking-guide.pdf</a></td>
</tr>
</tbody>
</table>

Dell EMC AMP-VX Product Guide 113
<table>
<thead>
<tr>
<th>Product</th>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware NSX 6.4 on the VxBlock System 1000 with AMP-VX</td>
<td>VMware NSX reproduces the entire network model in software, enabling a network topology to be created and provisioned in seconds.</td>
<td><a href="https://cpsdocs.dell">https://cpsdocs.dell</a> EMC.com/bundle/P_AO_NSX64</td>
</tr>
</tbody>
</table>