## Revision history

<table>
<thead>
<tr>
<th>Date</th>
<th>Document revision</th>
<th>Description of changes</th>
</tr>
</thead>
</table>
| June 2019      | 1.4               | - Added support for VMware vSphere 6.7.  
- Updated for VxBlock Central 1.0.  
- Updated for new VxBlock Central licensing. |
| December 2016  | 1.3               | Added support for the Cisco UCS C220 M4 Rack Server.  
Removed IPI appliance from sample configuration illustrations.  
Added support for AMP-2 on Cisco UCS C2x0 M4 servers with VMware vSphere 5.5. |
| April 2016     | 1.2               | Added support for VxBlock System 240, VMware vSphere 6.0, and AMP-2 enhancements for Cisco UCS M4 Servers.  
Added support for Cisco Nexus 3172TQ Switches. |
| August 2015    | 1.1               | Added IPI cabinet information                                                                                                                                 |
| August 2014    | 1.0               | Initial release                                                                                                                                                 |
Introduction

This document describes the high-level design of the VxBlock System 240 and the Vblock System 240, including the hardware and software components.

In this document, the VxBlock System and the Vblock System are referred to as Converged Systems.

Note: This document describes all the features and components supported on the Converged System. Some features or components may not exist on your Converged System.

Refer to the Glossary for terms, definitions, and acronyms.
System overview

System architecture and components

Converged Systems have the following features:

- Standardized cabinets with multiple North American and international power solutions
- Support for multiple features of the Dell EMC operating environment for VNX arrays
- Advanced Management Platform (AMP) for Converged System management
- Unified network architecture provides the option to leverage Cisco Nexus switches to support IP and SAN without the use of Cisco MDS switches

Converged Systems contain the following key hardware and software components:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Converged Systems management</td>
<td>Vision Intelligent Operations for Converged Systems or VxBlock Central for VxBlock Systems.</td>
</tr>
<tr>
<td></td>
<td>The following VxBlock Central options are available:</td>
</tr>
<tr>
<td></td>
<td>- The VxBlock Central Base option provides you with the VxBlock Central user interface to manage and monitor Converged Systems.</td>
</tr>
<tr>
<td></td>
<td>- The VxBlock Central Advanced Analytics option provides you access to VxBlock Central Operations capabilities to monitor the health status and metrics of supported Converged Systems with VMware vRealize Operations (vROps) Manager.</td>
</tr>
<tr>
<td>Virtualization and management</td>
<td>VMware vSphere ESXi</td>
</tr>
<tr>
<td></td>
<td>VMware vCenter Server</td>
</tr>
<tr>
<td></td>
<td>VMware Platform Services Controller (VMware vSphere 6.0)</td>
</tr>
<tr>
<td></td>
<td>VMware Single Sign-On (SSO) Service (VMware vSphere 5.5 and higher)</td>
</tr>
<tr>
<td></td>
<td>VMware vSphere Server Enterprise Plus</td>
</tr>
<tr>
<td></td>
<td>PowerPath/VE or VMware Native Multipathing (NMP)</td>
</tr>
<tr>
<td></td>
<td>Cisco Integrated Management Controller (CIMC)</td>
</tr>
<tr>
<td></td>
<td>Unisphere Manager</td>
</tr>
<tr>
<td></td>
<td>VNX Local Protection Suite</td>
</tr>
<tr>
<td></td>
<td>VNX Remote Protection Suite</td>
</tr>
<tr>
<td></td>
<td>VNX Application Protection Suite</td>
</tr>
<tr>
<td></td>
<td>VNX Fast Suite</td>
</tr>
<tr>
<td></td>
<td>VNX Security and Compliance Suite</td>
</tr>
<tr>
<td></td>
<td>Secure Remote Services (ESRS)</td>
</tr>
</tbody>
</table>
Resource | Components
---|---
| | • Cisco UCS C220 M3 and M4 Servers for AMP

**Compute**

- Cisco UCS C220 Server
- Cisco UCS Virtual Interface Card (VIC) 1225 or 1227

**Network**

- Cisco Nexus 5548UP Switches
- Cisco Nexus 3172TQ Switch or Cisco Nexus 3048 Switch
- (Optional) VMware Virtual Distributed Switch (VDS) (VMware vSphere 5.5 and higher)
- (Optional) Cisco Nexus 1000V Series Virtual Switches

**Storage**

- VNX5200 storage array

**Note:** The RCM 6.5 train, which supports VMware vSphere 6.5, does not support the Cisco Nexus 1000V Switch. Dell EMC recommends migrating virtual environment to the VMware Distributed Virtual Switch before the VMware vSphere 6.5 upgrade.

The following table summarizes the Converged System architecture:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot path</td>
<td>SAN</td>
</tr>
<tr>
<td>Cabinet</td>
<td>One 42 RU</td>
</tr>
<tr>
<td>Compute</td>
<td>Four to 12 Cisco UCS C220 M3 or Cisco UCS C220 M4 servers with one or two CPUs</td>
</tr>
<tr>
<td><strong>Memory options</strong></td>
<td></td>
</tr>
<tr>
<td>• 96 GB (3 x 32 GB) - Single CPU only</td>
<td></td>
</tr>
<tr>
<td>• 128 GB (4 x 32 GB) - Single and Dual CPU</td>
<td></td>
</tr>
<tr>
<td>• 192 GB (6 x 32 GB) - Single and Dual CPU</td>
<td></td>
</tr>
<tr>
<td>• 256 GB (8 x 32 GB) - Single and Dual CPU</td>
<td></td>
</tr>
<tr>
<td>• 384 GB (12 x 32 GB) - Single and Dual CPU</td>
<td></td>
</tr>
<tr>
<td>• 512 GB (16 x 32 GB) - Dual CPU only</td>
<td></td>
</tr>
<tr>
<td><strong>CPU options</strong></td>
<td></td>
</tr>
<tr>
<td>• E5-2630LEv4 (8 cores, 1.8 GHz)</td>
<td></td>
</tr>
<tr>
<td>• E5-2637Ev4 (4 cores, 3.5 GHz)</td>
<td></td>
</tr>
<tr>
<td>• E5-2650Ev2 (12 cores, 2.2 GHz)</td>
<td></td>
</tr>
<tr>
<td>Data store type</td>
<td>Block = VMFS</td>
</tr>
<tr>
<td></td>
<td>Unified = NFS and VMFS</td>
</tr>
<tr>
<td>Disk drives</td>
<td>Minimum configuration = 11</td>
</tr>
<tr>
<td></td>
<td>Maximum configuration = 105</td>
</tr>
<tr>
<td>Management switch</td>
<td>One Cisco Nexus 3172TQ Switch or one Cisco Nexus 3048 Switch</td>
</tr>
<tr>
<td>Storage access</td>
<td>Block or unified</td>
</tr>
</tbody>
</table>
## Feature Description

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage array</td>
<td>VNX5200 storage array</td>
</tr>
<tr>
<td>Storage back-end SAS buses</td>
<td>2</td>
</tr>
<tr>
<td>Storage capacity</td>
<td>• 25 drive DPE&lt;br&gt;• Two 25 drive DAEs for EFD and SAS drives&lt;br&gt;• Two 15 drive DAEs for NL-SAS drives</td>
</tr>
<tr>
<td>Storage protocol</td>
<td>Block = FC&lt;br&gt;Unified = FC, NFS, and CIFS</td>
</tr>
<tr>
<td>Unified Ethernet/SAN switches</td>
<td>Two Cisco Nexus 5548UP Switches for Ethernet and FC traffic</td>
</tr>
<tr>
<td>Unified storage X-Blades</td>
<td>0 or 2</td>
</tr>
<tr>
<td>Unified storage control stations</td>
<td>0 or 2</td>
</tr>
</tbody>
</table>

For information about certified versions of components, refer to the *Release Certification Matrix.*

## Base configurations and scaling

Converged Systems have base configurations that contain a minimum set of compute and storage components and fixed network resources that are integrated in a 19 inch, 42U cabinet.

You can customize the following hardware:

<table>
<thead>
<tr>
<th>Hardware</th>
<th>How it can be customized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compute servers</td>
<td>Four to twelve Cisco UCS C220 servers with CPU and memory configuration options.</td>
</tr>
<tr>
<td>Data Mover Enclosure (DME) packs</td>
<td>One DME (two X-Blades) and two control stations can be added as part of a unified storage addition.</td>
</tr>
<tr>
<td>Storage</td>
<td>VNX5200 storage array</td>
</tr>
<tr>
<td>Storage hardware</td>
<td>Drive flexibility for up to three tiers of storage per pool, drive quantities in each tier, the RAID protection for each pool, and the number of disk array enclosures (DAEs).</td>
</tr>
<tr>
<td>Supported disk drives</td>
<td>100/200/400 GB 2.5&quot; solid state drive (extreme performance)&lt;br&gt;600/900 GB 10K RPM 2.5&quot; SAS (performance)&lt;br&gt;2/3/4 TB 7.2 K RPM 3.5&quot; NL-SAS (capacity)</td>
</tr>
<tr>
<td>Supported RAID types</td>
<td>Tier 1: RAID 1/0 (4+4), RAID 5 (4+1) or (8+1), RAID 6 (6+2) or (14+2)&lt;br&gt;Tier 2: RAID 1/0 (4+4), RAID 5 (4+1) or (8+1), RAID 6 (6+2) or (14+2)&lt;br&gt;Tier 3: RAID 1/0 (4+4), RAID 5 (4+1) or (8+1), RAID 6 (6+2) or (14+2)</td>
</tr>
<tr>
<td>Management hardware</td>
<td>The second generation of the Advanced Management Platform (AMP-2) centralizes management of Converged System components. The default option for this platform is the virtual model (AMP-2V).</td>
</tr>
</tbody>
</table>
Together, the components offer balanced compute, I/O bandwidth, and storage capacity relative to the servers and storage arrays in the Converged System. All components have 1+1 or N+1 redundancy. These resources can be scaled up as necessary to meet increasingly stringent requirements.

Converged Systems are designed to keep hardware changes to a minimum if the storage protocol changes after installation (for example, from block storage to unified storage). Cabinet space is reserved for all components that are needed for each storage configuration, all fitting in a single 42U cabinet.

Related information

Management hardware components on page 31

AMP-2 is available on the VxBlock System 240 and Vblock System 240 with two AMP server models.

Scaling up compute resources on page 12

The Converged System contains from four to twelve Cisco UCS C220 servers.

Scaling up storage resources on page 16

This topic describes the RAID packs option and the disk array enclosures option for scaling up storage resources.

Storage overview on page 14

Connectivity overview

Components and connectivity in Converged Systems are conceptually subdivided into three layers:

<table>
<thead>
<tr>
<th>Layer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compute</td>
<td>Contains the components that provide the computing power in the Converged System and host the virtual machines. The Cisco UCS C220 Servers belong in this layer.</td>
</tr>
<tr>
<td>Network</td>
<td>Contains the components that provide switching and connectivity between the compute and storage layers in a Converged System and between the Converged System and the customer network. The Cisco Nexus 3172TQ or Cisco Nexus 3048 Switch and the Cisco Nexus 5548UP switches belong in this layer.</td>
</tr>
<tr>
<td>Storage</td>
<td>VNX5200 storage array</td>
</tr>
</tbody>
</table>

All components incorporate redundancy into the design.

The following illustration provides a high level overview of the components with redundant network connectivity:
Cisco UCS C220 server on page 12

The Cisco UCS C220 server is a high-density, two-socket, one rack unit (RU) rack-mount server that is built for production-level network infrastructure, web services, and mainstream data center, branch, and remote-office applications.

Network overview on page 19

The Converged System contains an Ethernet/SAN switch and a management switch that connects the components to each other and to external resources, such as backup and recovery servers and the customer network.

Storage overview on page 14
Compute layer hardware

Scaling up compute resources

The Converged System contains from four to twelve Cisco UCS C220 servers.
You can add Cisco UCS C220 servers, as needed, up to the maximum number of servers. Servers are added as needed, in single-server increments.

Related information
Base configurations and scaling on page 9
Converged Systems have base configurations that contain a minimum set of compute and storage components and fixed network resources that are integrated in a 19 inch, 42U cabinet.

Cisco UCS C220 server

The Cisco UCS C220 server is a high-density, two-socket, one rack unit (RU) rack-mount server that is built for production-level network infrastructure, web services, and mainstream data center, branch, and remote-office applications.

The Converged System contains from four to twelve Cisco UCS C220 servers.

The Cisco UCS C220 server provides:

- One or two processors
- The following CPU types:
  - E5-2680v2 (10 cores, 2.80 GHz, 115W)
  - E5-2630Lv2 (6 cores, 2.40 GHz, 60W)
  - E5-2637v2 (4 cores, 3.50 GHz, 130W)
- 64 GB, 96 GB, 128 GB, 192 GB, or 256 GB of memory. 192 GB and 256 GB of memory are supported only with two CPUs.
- Cisco UCS Virtual Interface Card (VIC) 1225 for converged networking
- Virtualization optimization

Cisco Trusted Platform Module

The Cisco Trusted Platform Module (TPM) is a computer chip that securely stores artifacts such as measurements, passwords, certificates, or encryption keys that are used to authenticate the Converged System. The Cisco TPM provides authentication and attestation services that enable safer computing in all environments.

The Cisco TPM is available by default in as a component within some Cisco UCS Blade Servers and Rack Servers and is shipped disabled.
Dell EMC supports Cisco TPM hardware but does not support the Cisco TPM functionality. Using Cisco TPM features involves using a software stack from a vendor with significant domain experience in trusted computing. Consult your software stack vendor for configuration and operational considerations relating to the Cisco TPMs.
VMware vSphere 6.7 supports TPM version 2.0.
Bare metal support policy

Since many applications cannot be virtualized due to technical and commercial reasons, Converged Systems support bare metal deployments, such as non-virtualized operating systems and applications.

While it is possible for Converged Systems to support these workloads (with the following caveats), due to the nature of bare metal deployments, Dell EMC can only provide reasonable effort support for systems that comply with the following requirements:

- Converged Systems contain only Dell EMC published, tested, and validated hardware and software components. The Release Certification Matrix provides a list of the certified versions of components for Converged Systems.
- The operating systems used on bare metal deployments for compute components must comply with the published hardware and software compatibility guides from Cisco and Dell EMC.
- For bare metal configurations that include other hypervisor technologies (Hyper-V, KVM, etc.) those hypervisor technologies are not supported by Dell EMC. Dell EMC support is provided only on VMware Hypervisors.

Dell EMC reasonable effort support includes Dell EMC acceptance of customer calls, a determination of whether a Converged System is operating correctly, and assistance in problem resolution to the extent possible.

Dell EMC is unable to reproduce problems or provide support on the operating systems and applications installed on bare metal deployments. In addition, Dell EMC does not provide updates to or test those operating systems or applications. The OEM support vendor should be contacted directly for issues and patches related to those operating systems and applications.
Storage layer hardware

Storage overview

The VNX series are fourth-generation storage platforms that deliver industry-leading capabilities. They offer a unique combination of flexible, scalable hardware design and advanced software capabilities that can meet the diverse needs of today’s organizations.

The VNX series platforms support block and unified storage. The platforms are optimized for VMware virtualized applications. They feature flash drives for extendable cache and high performance in the virtual storage pools. Automation features include self-optimized storage tiering and application-centric replication.

The storage array consists of up to five disk enclosures (DPEs and DAEs) that contain disk drives. These connect to dual storage processors (SPs) over six GB four-lane serial attached SCSI (SAS). Fibre Channel (FC) expansion cards within the storage processors connect to the Cisco Nexus 5548UP switches within the network layer over FC.

Regardless of the storage protocol implemented at startup (block or unified), cabinet space can accommodate cabling and power to support hardware expansion for these storage protocols. This arrangement makes it easier to move from block storage to unified storage with minimal hardware changes. However, all components must fit in the single 42U cabinet.

Note: All VNX components are installed in Dell EMC cabinets, in a Dell EMC-specific layout.

Related information

Base configurations and scaling on page 9
Converged Systems have base configurations that contain a minimum set of compute and storage components and fixed network resources that are integrated in a 19 inch, 42U cabinet.

Storage features support on page 15
This topic presents additional storage features available on the Converged System.

Replication

This section describes how Converged Systems can be upgraded to include RecoverPoint.

For block storage configurations, the Converged System can be upgraded to include RecoverPoint. This replication technology provides continuous data protection and continuous remote replication for on-demand protection and recovery to any point in time. RecoverPoint advanced capabilities include policy-based management, application integration, and bandwidth reduction. RecoverPoint is included in the Local Protection Suite and Remote Protection Suite.

To implement RecoverPoint within a Converged System, add two or more RecoverPoint Appliances (RPA) in a cluster to the Converged System. This cluster can accommodate approximately 80 MBps sustained throughput through each RPA.

To ensure proper sizing and performance of an RPA solution, Dell EMC works with a Technical Consultant. They collect information about the data to be replicated, as well as data change rates, data growth rates, network speeds, and other information that is needed to ensure that all business requirements are met.
## Storage features support

This topic presents additional storage features available on the Converged System.

### Support for array hardware or capabilities

The VNX operating environment supports the following features:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NFS Virtual X-Blades – VDM (Multi-LDAP Support)</strong></td>
<td>Provide security and segregation for service provider environmental clients.</td>
</tr>
<tr>
<td><strong>Data-in-place block compression</strong></td>
<td>When compression is enabled, thick LUNs are converted to thin LUNs and are compressed in place. RAID group LUNs are migrated into a pool during compression. There is no need for additional space to start compression. Decompression temporarily requires additional space, because it is a migration and not an in-place decompression.</td>
</tr>
</tbody>
</table>
| **Compression for file/display compression capacity savings** | Available file compression types:  
  - Fast compression (default)  
  - Deep compression (up to 30% more space efficient, but slower and with higher CPU usage)  
 Displays capacity savings due to compression to allow a cost/benefit comparison (space savings versus performance impact). |
| **VNX snapshots**                                            | VNX snapshots are for storage pools only, not for RAID groups. Storage pools can use SnapView snapshots and VNX snapshots at the same time.  
  __Note__: This feature is optional. Refer to Dell EMC best practices for different use cases of SnapView snapshots versus VNX snapshots. |
| **Correlated statistics enhancements**                       | Correlated statistics capture real-time statistics about I/O activity on VNX file storage. CIFS and NFS statistics are correlated by client IP addresses, CIFS/NFS users, and disk volumes.  
 The following indexes are added to the correlated statistical data:  
  - NFS groups (lists the 20 most active NFS groups for an X-Blade)  
  - NFS users (lists the 20 most active NFS users for an X-Blade)  
  - NFS file systems (lists the top 20 NFS operations per client per file system. This can be correlated by file system, client IP, or NFS operation).  
 CIFS statistics/file system statistics:  
  - Files in a quota tree (lists the 20 most active files in each quota tree) |
### Feature Description

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Files in a file system</td>
<td>Files in a file system (lists the 20 most active files in each file system).</td>
</tr>
<tr>
<td>NFS statistics: NFS exports</td>
<td>NFS exports (lists the 20 most active exports on an X-Blade)</td>
</tr>
<tr>
<td>NFS groups:</td>
<td></td>
</tr>
<tr>
<td>CIFS servers (by host name)</td>
<td>CIFS servers (lists the top 20 most active CIFS servers on an X-Blade)</td>
</tr>
<tr>
<td>CIFS clients (by host name)</td>
<td>CIFS clients (by host name)</td>
</tr>
</tbody>
</table>

### Hardware features

Dell EMC implements the following VNX features:
- Dual 10 Gigabit Ethernet Active Twinax IP IO/SLIC between the X-Blades and Cisco Nexus 5548UP Switches
- Utilization of 2½ inch vault drives
- 2½ inch and 3½ inch DAEs and drive form factors

### File deduplication

File deduplication is supported but is not enabled by default. Enabling this feature requires knowledge of capacity and storage requirements.

### Block compression

Block compression is supported but is not enabled by default. Enabling this feature requires knowledge of capacity and storage requirements.

### External NFS and CIFS access

The Converged System presents CIFS shares and NFS file systems to internal and external clients. CIFS shares and NFS file systems are connected to both internal virtual machines and to external client systems at the same time on a single share system. VMware NFS datastores are connected to both internal and external hosts, but not at the same time. If both internal and external NFS datastores are required, two NFS file systems must be created; one for internal hosts and one for external hosts.

### Snapshots

For block storage snapshots, SnapView is supported. This software provides local block replication using snaps and clones without the extra cost of the optional RecoverPoint Appliances. This software is included in the VNX Local Protection Suite.

For NAS file system snapshots, SnapSure is supported. It is included in the VNX Local Protection Suite.

VNX Snapshots creates point-in-time data copies.

### Replicas

For NAS configurations, VNX Replicator is supported. This software can create local clones (full copies) and replicate file systems asynchronously across IP networks. VNX Replicator is included in the VNX Remote Protection Suite.

### Scaling up storage resources

This topic describes the RAID packs option and the disk array enclosures option for scaling up storage resources.

To scale up storage resources, you can:
- Add RAID packs
Add disk array enclosures

Packs and disk array enclosures are added when Converged Systems are built and after they are deployed.

**RAID packs**

Storage capacity is increased by adding RAID packs. Each pack contains a number of drives of a given type, speed, and capacity. The number of drives in a pack depends on the RAID level that it supports.

The number and types of RAID packs included in Converged Systems are based on the following:

- The number of storage pools that are needed.
- The storage tiers that each pool contains, and the speed and capacity of the drives in each tier.

The following table lists tiers, supported drive types, and supported speeds and capacities.

<table>
<thead>
<tr>
<th>Tier</th>
<th>Drive type</th>
<th>Supported speeds and capacities</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Solid-state Enterprise Flash drives (EFD)</td>
<td>100 GB 2.5&quot;</td>
</tr>
<tr>
<td></td>
<td>(extreme performance)</td>
<td>200 GB 2.5&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>400 GB 2.5&quot;</td>
</tr>
<tr>
<td>2</td>
<td>Serial attached SCSI (SAS)</td>
<td>600 GB 10K RPM 2.5&quot;</td>
</tr>
<tr>
<td></td>
<td>(performance)</td>
<td>900 GB 10K RPM 2.5&quot;</td>
</tr>
<tr>
<td>3</td>
<td>Nearline SAS (capacity)</td>
<td>2 TB 7.2K RPM 3.5&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 TB 7.2K RPM 3.5&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 TB 7.2K RPM 3.5&quot;</td>
</tr>
</tbody>
</table>

- The RAID protection level for the tiers in each pool. The following table describes each supported RAID protection level. The RAID protection level for the different pools vary.

<table>
<thead>
<tr>
<th>RAID protection level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAID 1/0</td>
<td>- A set of mirrored drives.</td>
</tr>
<tr>
<td></td>
<td>- Offers the best overall performance of the three supported RAID protection levels.</td>
</tr>
<tr>
<td></td>
<td>- Offers robust protection. Can sustain double-drive failures that are not in the same mirror set.</td>
</tr>
<tr>
<td></td>
<td>- Lowest economy of the three supported RAID levels since usable capacity is only 50% of raw capacity.</td>
</tr>
<tr>
<td>RAID 5</td>
<td>- Block-level striping with a single parity block, where the parity data is distributed across all of the drives in the set.</td>
</tr>
<tr>
<td></td>
<td>- Offers the best mix of performance, protection, and economy.</td>
</tr>
<tr>
<td></td>
<td>- Has a higher write performance penalty than RAID 1/0 because multiple I/Os are required to perform a single write.</td>
</tr>
<tr>
<td></td>
<td>- With single parity, can sustain a single drive failure with no data loss. Vulnerable to data loss or unrecoverable read errors on a track during a drive rebuild.</td>
</tr>
<tr>
<td></td>
<td>- Highest economy of the three supported RAID levels. Usable capacity is 80% of raw capacity.</td>
</tr>
<tr>
<td>RAID 6</td>
<td>- Block-level striping with two parity blocks, distributed across all of the drives in the set.</td>
</tr>
<tr>
<td></td>
<td>- Offers increased protection and read performance comparable to RAID 5.</td>
</tr>
<tr>
<td></td>
<td>- Has a significant write performance penalty because multiple I/Os are required to perform a single write.</td>
</tr>
</tbody>
</table>
RAID protection level | Description
---|---
- Economy is very good. Usable capacity is 75% of raw capacity or better.
- Dell EMC best practice for SATA and NL-SAS drives.

There are RAID packs for each combination of RAID protection level and tier type. The RAID levels dictate the number of drives that are included in the packs. The following table lists RAID protection levels and the number of drives in the pack for each level: RAID 5 or RAID 1/0 is for performance and extreme performance tiers, and RAID 6 is for the capacity tier.

<table>
<thead>
<tr>
<th>RAID protection level</th>
<th>Number of drives per RAID pack</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAID 1/0</td>
<td>8 (4 data + 4 mirrors)</td>
</tr>
<tr>
<td>RAID 5</td>
<td>5 (4 data + 1 parity) or 9 (8 data + 1 parity)</td>
</tr>
<tr>
<td>RAID-6</td>
<td>8 (6 data + 2 parity) or 16 (14 data + 2 parity)</td>
</tr>
</tbody>
</table>

**Disk array enclosures**

If the number of RAID packs is expanded, more disk array enclosures (DAEs) might be required. DAEs are added individually. The base includes the DPE as the first DAE.

There are two types of DAEs: a 15 drive 3U enclosure for 3½ inch form factor drives and a 25 drive 2U enclosure for 2½ inch form factor drives. To ensure that the loads are balanced, physical disks will be spread across the DAEs in accordance with best practice guidelines.

**Related information**

**Base configurations and scaling** on page 9

Converged Systems have base configurations that contain a minimum set of compute and storage components and fixed network resources that are integrated in a 19 inch, 42U cabinet.

**Secure Remote Services**

This topic describes how Secure Remote Services (SRS) monitors the health of storage arrays.

SRS allows Dell EMC personnel to remotely monitor the health of storage arrays and perform support and maintenance functions. SRS serves as the conduit for all communications between Dell EMC and the storage arrays. SRS monitors the health of multiple storage arrays. SRS is integrated into the base software suite.

Detailed information about SRS is available at [support.emc.com](http://support.emc.com).
Network layer hardware

Network overview

The Converged System contains an Ethernet/SAN switch and a management switch that connects the components to each other and to external resources, such as backup and recovery servers and the customer network.

Ethernet/SAN switches

Two Cisco Nexus 5548UP Switches to provide Ethernet and Fibre Channel (FC) connectivity:

- Between the internal components.
- To the site network.
- To the redundant connections on the Cisco Nexus 3172TQ or Cisco Nexus 3048 switches.
- To Advanced Management Platform (AMP) through redundant connections between the AMP and the Cisco Nexus 5548UP switches.

The two Cisco Nexus 5548UP Switches support low latency line-rate 10 Gb Ethernet and 8 Gb FC connectivity on up to 32 ports. A unified port expansion module provides an extra 16 ports of 10 GbE or 8 Gb FC connectivity. The 16-port expansion module is dedicated for FC connectivity. The FC ports are licensed in packs of eight based on the demand.

Management switch

Cisco Nexus 3172TQ or Cisco Nexus 3048 Switches in the network layer provide IP connectivity between compute-layer components and storage-layer components. They also provide IP connectivity to the site network.

These switches provide configuration flexibility with LAN base, IP base, and IP services software.

Two 1/10 Gbps SFP+ uplink ports provide customer connectivity. Depending on the desired connection, 1GbE copper SFP+, 1GbE Fiber SFP+, or 10Gbe SFP+ transceivers are provided.

To facilitate the required level of redundancy and throughput, the customer network uplink device should support port aggregation.

Related information

Management hardware components on page 31
- AMP-2 is available on the VxBlock System 240 and Vblock System 240 with two AMP server models.

Management software components on page 32
- The AMP is delivered pre-configured with the following software tools:
Virtualization

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 6.0 includes a pair of Platform Service Controller Linux appliances to provide the SSO service. Either the VMware vCenter Service Appliance or the VMware vCenter Server for Windows can be deployed.

VMware vSphere 6.5 or VMware vSphere 6.7 includes a pair of Platform Service Controller Linux appliances to provide the SSO service. For VMware vSphere 6.5, VMware vSphere 6.7, and later releases, VMware vCenter Server Appliance is the default deployment model for vCenter Server.

VMware vSphere 6.7 deployments support embedded PSC deployment and is the default deployment mode.

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

Virtualization overview

VMware vSphere is the virtualization platform that provides the foundation for the private cloud. The core VMware vSphere components are the VMware vSphere Hypervisor ESXi and VMware vCenter Server for management. VMware vSphere 5.5, or higher includes a Single Sign-on (SSO) component. VMware vSphere 6.0 includes a pair of Platform Service Controller Linux appliances to provide the SSO service. Only VMware vSphere vCenter server on Windows is supported.

The hypervisors are deployed in a cluster configuration. The cluster allows dynamic allocation of resources, such as CPU, memory, and storage. The cluster also provides workload mobility and flexibility with the use of VMware vMotion and Storage vMotion technology. Either the VMware vCenter Service Appliance or the VMware vCenter Server for Windows can be deployed.

Related information

- **VMware vCenter Server (VMware vSphere 5.5 or 6.0) on page 21**
  
  VMware vCenter Server is a central management point for the hypervisors and virtual machines. VMware vCenter is installed on a 64-bit Windows Server and runs VMware Update Manager as a service to help manage host patches.

- **VMware vSphere Hypervisor ESXi on page 20**
  
  The VMware vSphere Hypervisor ESXi runs in the management servers and in Converged Systems using VMware vSphere Server Enterprise Plus.

**VMware vSphere Hypervisor ESXi**

The VMware vSphere Hypervisor ESXi runs in the management servers and in Converged Systems using VMware vSphere Server Enterprise Plus.

The VMware vSphere Hypervisor ESXi runs in the Advanced Management Platform (AMP) and in the Converged System using VMware vSphere Server Enterprise Plus.

This lightweight hypervisor requires very little space to run (less than 6 GB of storage required to install) and has minimal management overhead.

VMware vSphere ESXi does not contain a console operating system. The VMware vSphere Hypervisor ESXi boots from Cisco FlexFlash (SD card) on the AMP. For the compute blades, ESXi boots from the SAN through an independent Fibre Channel (FC) LUN presented from the VNX storage array. The FC LUN also contains the hypervisor’s locker for persistent storage of logs and other diagnostic files to provide stateless computing within Converged Systems. The stateless hypervisor is not supported.
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 virtual machines (VMs). Clusters can scale up to a maximum of 32 hosts for VMware vSphere 5.5 and 64 hosts for VMware vSphere 6.0. Clusters can support thousands of VMs.

The clusters can also support a variety of Cisco UCS C-Series servers running inside the same cluster.

Note: Some advanced CPU functionality might be unavailable if more than one CPU model is running a cluster.

Datastores

Converged Systems support a mixture of datastore types: block level storage using VMFS or file level storage using NFS.

The maximum size per VMFS5 volume is 64 TB (50 TB VMFS3 @ 1 MB). VMware 5.5 and higher limits the VMDK file size to 62TB. Each host/cluster supports a maximum of 255 volumes.

Dell EMC optimizes the advanced settings for VMware vSphere ESXi hosts that are deployed in Converged Systems to maximize the throughput and scalability of NFS data stores. Converged Systems support a maximum of 256 NFS datastores per host.

Virtual networks

Virtual networking in the AMP uses the standard virtual switches. The Cisco Nexus 1000V distributed virtual switch manages virtual networking and ensures consistent, policy-based network capabilities to all servers in the data center by allowing policies to move with a VM during live migration. This provides persistent network, security, and storage compliance.

Alternatively, with VMware 5.5 and later, virtual networking in Converged Systems is managed by a VMware vCenter Virtual Distributed Switch with comparable features to the Cisco Nexus 1000V where applicable. The VMware VDS option consists of both a VMware Standard Switch (VSS) and a VMware vSphere Distributed Switch (VDS) and uses a minimum of four uplinks presented to the hypervisor.

The implementation of Cisco Nexus 1000V Series Switch and VMware VDS for VMware vSphere use intelligent network Class of Service (CoS) marking and Quality of Service (QoS) policies to appropriately shape network traffic according to workload type and priority. With VMware vSphere 6.0, QoS is set to Default (Trust Host). The vNICs are equally distributed across all available physical adapter ports to ensure redundancy and maximum bandwidth where appropriate. This provides general consistency and balance across all Cisco UCS blade models, regardless of the Cisco UCS Virtual Interface Card (VIC) hardware. Thus, VMware vSphere ESXi has a predictable uplink interface count. All applicable VLANs, native VLANs, MTU settings, and QoS policies are assigned to the virtual network interface cards (vNIC) to ensure consistency in case the uplinks need to be migrated to the VMware vSphere Distributed Switch (VDS) after manufacturing.

Related information

Management hardware components on page 31
AMP-2 is available on the VxBlock System 240 and Vblock System 240 with two AMP server models.

Management software components on page 32
The AMP is delivered pre-configured with the following software tools:

VMware vCenter Server (VMware vSphere 5.5 or 6.0)

VMware vCenter Server is a central management point for the hypervisors and virtual machines. VMware vCenter is installed on a 64-bit Windows Server and runs VMware Update Manager as a service to help manage host patches.

VMware vCenter Server 5.5 resides on a 64-bit Windows Server. VMware vCenter Server 6.0 is preferred to reside on the VMware vCenter Server Appliance (vCSA) or alternatively on a 64-bit Windows Server.
VMware Update Manager 5.5 and 6.0 reside on a 64-bit Windows Server. VMware Update Manager may have an embedded instance of Microsoft SQL Server if vCSA is in use. VMware Update Manager runs as a service to assist with host patch management.

VMware vCenter server allows you to perform the following:

- Clone VMs
- Create templates
- Perform VMware vMotion and VMware Storage vMotion
- Configure the VMware Distributed Resource Scheduler (DRS) and VMware vSphere high-availability clusters

VMware vCenter Server also provides monitoring and alerting capabilities for hosts and VMs. System administrators can create and apply alarms to all managed objects in VMware vCenter Server, including:

- Data center, cluster, and host health, inventory, and performance
- Datastore health and capacity
- VM usage, performance, and health
- Virtual network usage and health

**Virtual Advanced Management Platform (AMP-2V)**

The Virtual Advanced Management Platform (AMP-2V) resides in a vAPP located across two nondedicated compute servers. The virtual AMP shares resources with other production workloads for hardware cost efficiency.

**Databases**

The backend database that supports VMware vCenter Server and VMware Update Manager (VUM) is remote Microsoft SQL Server 2012 for vSphere 5.5/6.0. If the AMP-2 with Cisco UCS M4 servers and VMware vSphere 6.0 is deployed with the default vCSA, the vCSA will use its own internal database. The SQL Server service requires a dedicated service account.

**Authentication**

VMware vCenter Single Sign-On (SSO) Service integrates multiple identity sources including Active Directory, Open LDAP, and local accounts for authentication. VMware SSO is available in VMware vSphere 5.5. VMware vSphere 6.0 includes a pair of Platform Service Controller Linux appliances to provide the SSO service. VMware vCenter Server, Inventory, Web Client, SSO, Core Dump Collector, and Update Manager run as separate Windows services. Each service, can be configured to use a dedicated service account, depending on the security and directory services requirements.

**Dell EMC supported features**

Dell EMC supports the following VMware vCenter Server features:

- VMware Single Sign-On (SSO) Service (VMware vSphere 5.5)
- VMware Platform Service Controller (VMware vSphere 6.0)
- VMware vSphere Web Client (used with VxBlock Central)
- VMware vCenter vSphere Distributed Switch (VDS)
- VMware vSphere High Availability
- VMware DRS
- VMware Fault tolerance
- VMware vMotion (Layer 3 capability available for compute resources (VMware vSphere 6.0))
- VMware Storage vMotion
- Raw device mappings
Virtualization

- Resource pools
- Storage DRS (capacity only)
- Storage-driven profiles (user-defined only)
- Distributed power management (up to 50 percent of VMware vSphere ESXi hosts/servers)
- VMware Syslog service
- VMware Core Dump Collector service

VMware vCenter Server (VMware vSphere 6.x)

VMware vCenter Server is a central management point for the hypervisors and VMs. VMware vCenter Server 6.5 or 6.7 resides on the VMware vCenter Server Appliance (vCSA).

By default, VMware vCenter Server is deployed using the VMware vCSA. VMware Update Manager (VUM) is fully integrated with the VMware vCSA and runs as a service to assist with host patch management.

AMP

AMP and the Converged System have a single VMware vCSA instance. VMware vCenter Server provides the following functionality:
- Cloning of VMs
- Creating templates
- VMware vMotion and VMware Storage vMotion
- Initial configuration of VMware Distributed Resource Scheduler (DRS) and VMware vSphere high-availability clusters

VMware vCenter Server provides monitoring and alerting capabilities for hosts and VMs. Converged System administrators can create and apply the following alarms to all managed objects in VMware vCenter Server:
- Data center, cluster and host health, inventory, and performance
- Data store health and capacity
- VM usage, performance, and health
- Virtual network usage and health

Databases

The VMware vCSA uses the embedded PostgreSQL database. The VMware Update Manager and VMware vCSA share the same PostgreSQL database server, but use separate PostgreSQL database instances.

Authentication

Converged Systems support the VMware Single Sign-On (SSO) Service capable of the integration of multiple identity sources including AD, Open LDAP, and local accounts for authentication. VMware vSphere 6.5 or 6.7 includes a pair of VMware Platform Service Controller (PSC) Linux appliances to provide the VMware SSO service. VMware vCenter Server, Inventory, Web Client, SSO, Core Dump Collector, and Update Manager run as separate services. Each service can be configured to use a dedicated service account depending on the security and directory services requirements.

Supported features

Dell EMC supports the following VMware vCenter Server features:
- VMware SSO Service
- VMware vSphere Platform Service Controller
- VMware vSphere Web Client (used with Vision Intelligent Operations or VxBlock Central)
- VMware vSphere Distributed Switch (VDS)
- VMware vSphere High Availability
- VMware DRS
- VMware Fault Tolerance
- VMware vMotion
- VMware Storage vMotion - Layer 3 capability available for compute resources, version 6.0 and higher
- Raw Device Mappings
- Resource Pools
- Storage DRS (capacity only)
- Storage driven profiles (user-defined only)
- Distributed power management (up to 50 percent of VMware vSphere ESXi hosts/blades)
- VMware Syslog Service
- VMware Core Dump Collector
- VMware vCenter Web Client

Dell EMC supports the following additional VMware vCenter Server features with VMware vSphere 6.7:
- Embedded deployment
- Embedded linked mode
- VMware vCenter High Availability with embedded PSC deployment
- VMware vSphere HTML5 Client
Management

VxBlock Central options

VxBlock Central is available in the modular offerings of Base, VxBlock Central Workflow Automation, and VxBlock Central Advanced Analytics to manage your Converged Systems.

VxBlock Central Base option

The Base option enables you to monitor the health and compliance of VxBlock Systems through a central dashboard. VxBlock System health is a bottom-up calculation that monitors health or operational status of the following:

- The VxBlock System as a whole system.
- The physical components such as a chassis, disk array enclosure, fan, storage processor, or X-Blade.
- The compute, network, storage, and management components that logically group the physical components.

The landing page of VxBlock Central provides a view of the health and compliance of multiple VxBlock Systems. You can run a compliance scan on one or more VxBlock Systems. You can view key performance indicators (KPI) for one or more components.

VxBlock Central contains dashboards that allow you to:

- View all components for selected VxBlock Systems, including detailed information such as serial numbers, IP address, firmware version, and location.
- View compliance scores and security and technical scan risks.
- View and compare RCMs on different systems.
- View real-time alerts for your system including severity, time, the system where the alert occurred, the ID, message, and status.
- Configure roles with AD integration.

The following table describes each dashboard:

<table>
<thead>
<tr>
<th>Dashboard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory</td>
<td>Provides high-level details of the components that are configured in a single view. It provides the name, IP address, type, and element manager, RCM scan results, and alert count for components. An inventory item can be selected to suppress alerts and enable alerts. When alerts are suppressed for a specific component, real-time alert notifications are suspended. You can search VxBlock Systems for specific components or subcomponents and export a spreadsheet of your search.</td>
</tr>
</tbody>
</table>
| RCM       | Provides the compliance score, security, and technical risks associated with each VxBlock System. From the dashboard, you can:  
- View noncompliant components, security, and technical risks associated for components.  
- Download software and firmware for your VxBlock System components to upgrade to a new RCM or remediate drift from your current RCM.  
- Run compliance scans and download and assess the results.  
- Check the base profile to determine whether components have the correct firmware versions.  
- Upload and install the latest compliance content. |
<table>
<thead>
<tr>
<th>Dashboard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Customize the compliance profile.</td>
</tr>
<tr>
<td>Alerts</td>
<td>Provides real-time System Alerts to monitor and receive alerts for critical failures on compute, storage, and network components. Administrators and Dell EMC Support can respond faster to incidents to minimize any impact of failures. Using the predefined alert notification templates to create alert notification profiles, you can specify how you want to be notified for a critical alert.</td>
</tr>
<tr>
<td>Roles</td>
<td>When VxBlock Central is integrated with Active Directory (AD), VxBlock Central authenticates AD users and supports mapping between AD groups and roles. Role mappings control the actions that a user is authorized to perform. By mapping an AD group to a role, you can control user permissions. When an AD user logs in to VxBlock Central, role mappings are checked for AD groups to which the user is assigned. The set of available permissions depends on the roles mapped to the groups in which the user is a member.</td>
</tr>
<tr>
<td>Advanced Management</td>
<td>Provides access to VxBlock Central Workflow Automation and VxBlock Central Advanced Analytics features.</td>
</tr>
</tbody>
</table>

**VxBlock Central Advanced Analytics option**

The Advanced Analytics option provides features that simplify operations you must perform for VxBlock Systems through advanced monitoring, system analytics, and simplified capacity management.

VMware vRealize Operations (vROps) Manager integration with VxBlock Central presents the topology and relationship of VxBlock Systems with compute, storage, network, virtualization, and management components. Advanced Analytics provides advanced monitoring, system analytics, and simplified capacity management through integration with VMware vROps Manager.

Advanced Analytics allows you to:

- Monitor health, performance, and capacity through predictive analytics.
- Troubleshoot and optimize your environment through alerts and recommended actions.
- Manage inventory and create reports.
- Define custom alerts for performance and capacity metrics in the following actions:
  - Collect data from VxBlock Systems every 15 minutes by default.
  - Collect real-time alerts from VxBlock Systems every three minutes, by default.
  - View VxBlock Central VM relationships to physical infrastructure. Core VM, MSM VM, and MSP VM resource monitoring enables you to identify and monitor a collection of resources associated with a VM.

The following illustration provides an overview of how VxBlock Central uses VMware vRealize:
VxBlock Central architecture

VxBlock Central uses VMs to provide services.

The following table provides an overview of VxBlock Central VMs:

<table>
<thead>
<tr>
<th>VM</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core</td>
<td>Discovers and gathers information about the inventory, location, and health of the VxBlock System.</td>
</tr>
<tr>
<td>MSM</td>
<td>Provides functions to manage multiple VxBlock Systems. In a data center environment, one MSM VM can be associated with up to 8 Core VMs.</td>
</tr>
<tr>
<td>MSP (optional)</td>
<td>Provides functions for RCM content prepositioning.</td>
</tr>
</tbody>
</table>

VxBlock Central includes the Core VM and the multisystem management (MSM) VM as a minimum configuration. The multisystem prepositioning (MSP) VM deployment is optional for prepositioning.

Discovery

The discovery model resides in a database and is exposed through REST and SNMP interfaces. Initial discovery is performed during manufacturing of the VxBlock System and relies on an .XML file that contains build and configuration information.
information. Core VM uses the .XML file to populate basic information about the VxBlock System and establish communication with components.

After initial discovery, Core VM uses the following methods to discover the VxBlock System, including physical components and logical entities:

- XML API
- SNMP
- SMI-S
- Vendor CLIs, such as Unisphere CLI
- Platform Management Interface

Core VM performs discovery every 15 minutes, by default. This setting can be changed as desired.

The following illustration is a high-level overview of integration between Core VM and various products and protocols:

**Data collection**

VxBlock Central uses data collectors to unzip required data from various web services.
The following table describes the data collectors:

<table>
<thead>
<tr>
<th>Data collector</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VxBlock Central collector</td>
<td>Uses the VxBlock Central REST API to collect the VxBlock System configuration data and key performance indicators (KPI) already discovered in Core VM. The configuration is stored with KPI data from Core VM into the Cassandra and Elasticsearch databases.</td>
</tr>
<tr>
<td>SMI-S collector</td>
<td>Works with the CIM Object Manager (ECOM) service that runs on SMI components to discover metrics for VMAX:</td>
</tr>
<tr>
<td></td>
<td>• Storage array</td>
</tr>
<tr>
<td></td>
<td>• Storage processor</td>
</tr>
<tr>
<td></td>
<td>• Storage volume</td>
</tr>
<tr>
<td></td>
<td>• Storage pool</td>
</tr>
<tr>
<td></td>
<td>• Storage tier</td>
</tr>
<tr>
<td></td>
<td>• Disk</td>
</tr>
<tr>
<td>SNMP collector</td>
<td>Collects information from SNMP enabled devices such as Cisco Nexus and MDS switches to discover metrics. Information can be collected from the following network components:</td>
</tr>
<tr>
<td></td>
<td>• Switches</td>
</tr>
<tr>
<td></td>
<td>• Network chassis</td>
</tr>
<tr>
<td></td>
<td>• Container</td>
</tr>
<tr>
<td></td>
<td>• Fan</td>
</tr>
<tr>
<td></td>
<td>• Expansion module</td>
</tr>
<tr>
<td></td>
<td>• Power supply bay</td>
</tr>
<tr>
<td></td>
<td>• PSU</td>
</tr>
<tr>
<td></td>
<td>• Network temperature sensor</td>
</tr>
<tr>
<td></td>
<td>• SFP</td>
</tr>
<tr>
<td></td>
<td>• IPI appliance</td>
</tr>
<tr>
<td>vSphere API collector</td>
<td>Works with VMware vCenter Server using the VMware vSphere API to discover metrics, for datastores, disk partitions, and clusters.</td>
</tr>
<tr>
<td>Dell EMC Unity REST collector</td>
<td>Collects configuration data from a Dell EMC Unity storage array and its components.</td>
</tr>
<tr>
<td>XIO REST collector</td>
<td>Collects metrics for storage array, storage volume, disk, and port. VxBlock Central collects all other configuration information with the collector.</td>
</tr>
<tr>
<td>XML API collector</td>
<td>Collects information from the Cisco UCS using the XML API to discover metrics.</td>
</tr>
<tr>
<td>VMware NSX collector</td>
<td>Collects information about VMware NSX components, such as Virtual Appliance Management and the NSX controllers. The NSX collector interfaces with the NSX Manager APIs.</td>
</tr>
</tbody>
</table>

**VxBlock Central Shell**

The VxBlock Central Shell removes the complexity of working with individual component interfaces and provides a plug-in structure that can be extended to include more functionality. VxBlock Central Shell creates an abstraction layer that removes the burden of having to use different login credentials, IP addresses, and syntax to make configuration changes across multiple components. VxBlock Central Shell can help manage multiple VxBlock Systems.
For example, to update the NTP server IP addresses for all switches on a VxBlock System, you can issue a single command without having to log in to each component.

```bash
> ntp switch set ['10.1.139.235', '10.1.219.13']
[Switch 'N5B' at 10.1.139.23:, result: ['10.1.139.235', '10.1.219.13'],
 Switch 'N5A' at 10.1.139.22:, result: ['10.1.139.235', '10.1.219.13'],
 Switch 'MGMT-N3B' at 10.1.139.2:, result: ['10.1.139.235', '10.1.219.13'],
 Switch 'MGMT-N3A' at 10.1.139.1:, result: ['10.1.139.235', '10.1.219.13'],
 Switch 'N1A' at 10.1.140.235:, result: ['10.1.139.235', '10.1.219.13'],
 Switch 'M9A' at 10.1.139.20:, result: ['10.1.139.235', '10.1.219.13'],
 Switch 'M9B' at 10.1.139.21:, result: ['10.1.139.235', '10.1.219.13']]
```

The shell is a framework layer built on top of Python and VxBlock CentralAPI bindings. In addition to the commands provided, any valid Python command can be run in the shell.

Developers writing extensions for the VxBlock Central Shell can provide a single interface for all components and enable users to:

- Perform operations on each VxBlock System as a single logical entity rather than a collection of components.
- Configure and manage settings at the individual VxBlock System component level.

**Secure Remote Services**

VxBlock Central can connect to Secure Remote Services (SRS) to automatically send system inventory, real-time alerts, and RCM fitness information through the SRS connection to collect and analyze data. Customers on VxBlock Central Version 1.5 and earlier use VxBlock Central Shell SRS Extension Pack to configure SRS.

Use the appropriate procedure to perform the following functions:

- Configure VxBlock Central to use SRS.
- Deregister VxBlock Central with SRS.
- Update a SRS gateway configuration or VxBlock Central ID (SWID).
- Uploads the following information to SRS about your Converged System:
  - Release Certification Matrix (RCM) compliance scan results (ZIP file containing CSV, XLS, PDF, and XML files) if you have installed RCM content and selected a default profile.
  - Converged System inventory files (JSON).
  - Converged System real-time alerts are automatically sent to SRS if notification is configured.
- Modify the schedule VxBlock Central uses to regularly send RCM and inventory information to SRS (only in VxBlock Central Version 1.5 and earlier).

**Key performance indicators**

Access key performance indicator (KPI) information using VxBlock Central or MSM VM. VxBlock Central displays charts and graphs of KPI information for the selected element type.

The following table provides examples of KPI information:

<table>
<thead>
<tr>
<th>Element type</th>
<th>Examples of KPI information</th>
</tr>
</thead>
<tbody>
<tr>
<td>storagearray</td>
<td>Remaining raw capacity</td>
</tr>
<tr>
<td></td>
<td>Total space available for user data</td>
</tr>
<tr>
<td></td>
<td>Remaining managed space</td>
</tr>
<tr>
<td></td>
<td>Total IO per second</td>
</tr>
<tr>
<td>storagepool</td>
<td>User capacity</td>
</tr>
<tr>
<td>disk</td>
<td>Disk raw capacity</td>
</tr>
<tr>
<td>Element type</td>
<td>Examples of KPI information</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td></td>
<td>Bandwidth</td>
</tr>
<tr>
<td>switch</td>
<td>Current bandwidth</td>
</tr>
<tr>
<td></td>
<td>Number of error inbound packets</td>
</tr>
<tr>
<td>rack</td>
<td>Monitor total energy.</td>
</tr>
<tr>
<td></td>
<td>Monitor average power consumption.</td>
</tr>
<tr>
<td>computeserver</td>
<td>Total memory</td>
</tr>
<tr>
<td></td>
<td>Temperature</td>
</tr>
</tbody>
</table>

The MSM VM API for multisystem services retrieves the following KPI data:

- All existing KPI definitions in the VxBlock System.
- Existing KPI definitions for a particular element type and/or component category.
- Time series KPI data:
  - A particular time resolution.
  - A start time for time series queries.
  - An end time for time series queries.

### Management components overview

The Advanced Management Platform (AMP) is a management system that includes the hardware and software to run Core Management and Dell EMC Optional workloads. The Core Management Workload is the minimum set of software required to install, operate, and support a Converged System, including hypervisor management, element managers, virtual networking components (Cisco Nexus 1000V switch or the Virtual Distributed Switch (VDS)), and VxBlock Central Software.

The AMP provides a single management point for the Converged System and provides the ability to:

- Run the Core Management and Optional workloads
- Monitor and manage Converged System health, performance, and capacity
- Provide network and fault isolation for management
- Eliminate resource overhead

### Management hardware components

AMP-2 is available on the VxBlock System 240 and Vblock System 240 with two AMP server models.

The following list shows the operational relationship for the AMP-2 design between Cisco UCS Servers and VMware vSphere:

- Cisco UCS C220 M3 server configured with VMware vSphere 5.5 or 6.0
- Cisco UCS C220 M4 server configured with VMware vSphere 5.5 or 6.0 (AMP-2P only)

The AMP options for the Converged System are explained in the following table:
### AMP option

<table>
<thead>
<tr>
<th>AMP option</th>
<th>Physical server</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMP-2V</td>
<td>Two Cisco UCS 220 servers with shared storage (runs within a vAPP)</td>
<td>AMP-2V, available by default, provides a highly available management platform that resides in the vAPP. AMP-2V uses nondedicated Cisco UCS 220 servers to run management workload applications that are shared with other workloads on the Converged System.</td>
</tr>
<tr>
<td>AMP-2P M3/M4</td>
<td>One Cisco UCS C220 server</td>
<td>AMP-2P is an optional configuration that uses a dedicated Cisco UCS C220 server to run management workloads applications. AMP-2P uses its own resources, not customer resources.</td>
</tr>
</tbody>
</table>

1. **Note:** In this document, the virtual AMP and the physical AMP are referred to as AMP-2V and AMP-2P.

### Related information

**Base configurations and scaling on page 9**

Converged Systems have base configurations that contain a minimum set of compute and storage components and fixed network resources that are integrated in a 19 inch, 42U cabinet.

### Management software components

The AMP is delivered pre-configured with the following software tools:

- Microsoft Windows Server 2008 Standard R2 SP1 x64
- Microsoft Windows Server 2012 R2 Standard x64
  1. **Note:** The AMP includes the licenses in the vAPP.
- VMware vSphere Server Enterprise Plus (VMware vSphere 5.5 and higher) (uses PSC for VMware vSphere 6.0)
  1. **Note:** The AMP uses existing licenses for the production workload of the Converged System.
- VMware vSphere Hypervisor ESXi
- VMware Single Sign-On (SSO) Service (VMware vSphere 5.5 and higher)
- VMware vSphere Web Client
- VMware VMware vCenter Server
  1. **Note:** For VMware vSphere 5.5, only VMware vSphere vCenter with Windows is supported.
  - For VMware vSphere 6.0, the default instance is created using VMware vCenter Server Appliance.
  - For VMware vSphere 6.0, an alternate instance can be created using Microsoft Windows.
  - Only one of these options can be implemented.
- VMware vCenter Database using Microsoft SQL Server 2012 Standard for vSphere 5.5 and higher
- VMware vCenter Update Manager
  - For VMware vSphere 5.5, the SQL server is a dedicated VM.
  - For VMware vSphere 6.0, the default configuration embeds the Microsoft SQL Server on same VM as the VUM.
  - For VMware vSphere 6.0, an alternate configuration leverages the remote Microsoft SQL Server with VMware vCenter Server.
  - Only one of these options can be implemented.
- VMware vSphere client
- VMware Platform Services Controller (VMware vSphere 6.0)
- Virtual networking component (Cisco Nexus 1000V switch or VMware Virtual Distributed Switch (VDS))
Converged Systems using VMware VDS do not include Cisco Nexus 1000V VSM VMs and vice versa.

- PowerPath/VE License Management Server
- Secure Remote Services (ESRS)
- Array management modules
- Cisco Device Manager and Cisco Data Center Network Manager
- (Optional) RecoverPoint software that includes RecoverPoint Management Application and RecoverPoint Deployment Manager
- (Optional) Cisco Secure Access Control Server (ACS)

**AMP software components (VMware vSphere 5.5 and 6.0)**

AMPs are delivered with specific installed software components that depend on the selected Release Certification Matrix (RCM).

**AMP-2 software components**

The following components are installed:

- Microsoft Windows Server 2008 R2 SP1 Standard x64
- Microsoft Windows Server 2012 R2 Standard x64
- VMware vSphere Enterprise Plus
- VMware vSphere Hypervisor ESXi
- VMware Single Sign-On (SSO) Service
- VMware vSphere Platform Services Controller
- VMware vSphere Web Client Service
- VMware vSphere Inventory Service
- VMware vCenter Server Appliance

**Note:** For VMware vSphere 5.5, only VMware vSphere vCenter with Windows is supported.

- VMware vCenter Database using Microsoft SQL Server 2012 Standard Edition
- VMware vCenter Update Manager (VUM) - Integrated with VMware vCenter Server Appliance

**Note:** For VMware vSphere 6.0, the preferred configuration (with VMware vSphere vCenter Server Appliance) embeds the SQL server on the same VM as the VUM. The alternate configuration leverages the remote SQL server with VMware vCenter Server on Windows. Only one of these options can be implemented.

- VMware vSphere client
- VMware vSphere Syslog Service (optional)
- VMware vSphere Core Dump Service (optional)
- VMware vSphere Distributed Switch (VDS)
- PowerPath/VE Management Appliance (PPMA)
- Secure Remote Support (SRS)
- Array management modules, including but not limited to
- Cisco Prime Data Center Network Manager and Device Manager
AMP software components (VMware vSphere 6.5 and 6.7)

AMPs are delivered with specific installed software components dependent on the selected Release Certification Matrix (RCM).

The following components are installed dependent on the selected RCM:

- Microsoft Windows Server 2008 R2 SP1 Standard x64 (AMP-2)
- Microsoft Windows Server 2012 R2 Standard x64
- VMware vSphere Enterprise Plus
- VMware vSphere Hypervisor ESXi
- VMware Single Sign-On (SSO) Service
- VMware vSphere Platform Services Controller (PSC)
- VMware vSphere Web Client Service
- VMware vSphere HTML5 Client Service
- VMware vSphere Inventory Service
- VMware vCenter Server Appliance (vCSA)
  
  Note: For VMware vSphere 6.5 or 6.7, only the VMware vSphere vCenter Server Appliance deployment model is offered.

- VMware vCenter Update Manager (VUM – Integrated with VMware vCenter Server Appliance)
- VMware vSphere Web Client (Flash/Flex client)
- VMware Host client (HTML5 based) for VMware vSphere 6.7
- VMware vSphere Syslog Service (optional)
- VMware vSphere Core Dump Service (optional)
- VMware vSphere Distributed Switch (VDS)
- PowerPath/VE Management Appliance (PPMA)
- Secure Remote Support
- Array management modules
- Cisco Prime Data Center Network Manager and Device Manager (DCNM)
- (Optional) RecoverPoint management software that includes the management application and deployment manager
- Embedded VMware PSCs
- VMware vCenter HA
Management network connectivity

AMP-2V network connectivity

AMP-2V is the virtual version of the Advanced Management Platform. It runs Core Management and Dell EMC Optional Workloads as virtual machines on customer resources.

Converged System AMP-2V connectivity rules

- AMP-2V uses the first two compute servers and leverages two 1 Gb ports on the Management Switch (shared Cisco Integrated Management Controller (CIMC)) and one 10 Gb port on each Cisco Nexus 5548UP Switch.
- Connect uplinks exist from each Cisco Nexus 5548UP Switch into the customer network for VLAN 105 only.
- Connect uplinks exist from the management switch into the customer management network for VLAN 101 only.
- All networks, except VLAN 101, are owned by the Cisco Nexus 5548UP Switches.
- The VMware VMkernel default gateway is on VLAN 105.

AMP-2V, VMware vSphere 5.5 or 6.0, and Cisco UCS C220 M3 servers

The following illustration provides an overview of the network connectivity for the AMP-2V with VMware vSphere 5.5 or 6.0, and the Cisco UCS C220 M3 server:
Note: This illustration reflects the connections between the devices, not the quantity of those connections.

The following illustrations show several VM server assignments.

Note: Converged Systems using VMware Virtual Distributed Switch (VDS) do not include Cisco Nexus1000V VSM VMs.

The following illustration shows AMP-2V with VMware vSphere 5.5 and the Single Sign-on (SSO) Service on Cisco UCS C220 M3 servers:
The following illustration shows the AMP-2V with VMware vSphere 6.0 and the Platform Services Controller on Cisco UCS C220 M3 servers:
AMP-2V, VMware vSphere 5.5 or 6.0, and Cisco UCS C220 M4 servers

The following illustration provides an overview of the network connectivity for the AMP-2V with VMware vSphere 5.5 or 6.0, and the Cisco UCS C220 M4 server:
Note: This illustration reflects the connections between the devices, not the quantity of those connections.

The following illustrations show VM server assignments.

Note: Converged Systems using VMware Virtual Distributed Switch (VDS) do not include Cisco Nexus1000V VSM VMs.

The following illustration shows AMP-2V with VMware vSphere 5.5 and the Single Sign-on (SSO) Service on Cisco UCS C220 M4 servers:
The following illustration shows the AMP-2V with VMware vSphere 6.0 and the Platform Services Controller on Cisco UCS C220 M4 servers:

The following illustration shows the AMP-2V with VMware vSphere 6.0 and the VMware vCenter Server Virtual Appliance on Cisco UCS C220 M4 servers:
AMP-2P network connectivity

AMP-2P is the minimum physical version of then Advanced Management Platform. It provides a single dedicated server running Core Management and Dell EMC Optional Management Workloads as virtual machines using its own resources, not customer resources.

AMP-2P connectivity rules

- AMP-2P has a single dedicated server that leverages three 1 Gb ports on the management switch (dedicated Cisco Integrated Management Controller (CIMC)) and one 10 Gb port on each Cisco Nexus 5548UP Switch.
- Connect uplinks exist from each Cisco Nexus 5548UP Switch into the customer network for VLAN 105 only.
- Connect uplinks exist from the management switch into the customer management network for VLAN 101 only.
- All networks, except VLAN 101, are owned by the Cisco Nexus 5548UP Switches. The VMware VMKernel default gateway is on VLAN 105.

AMP-2P, VMware vSphere 6.0 and Cisco UCS C220 M4 servers network connectivity

The following illustration shows the network management connectivity for AMP-2P with VMware vSphere 6.0 with Cisco UCS C220 M4 servers:
AMP-2P, VMware vSphere 6.0 and Cisco UCS M3 or M4 servers with PSCs VM server assignments

The following illustration shows the AMP-2P with VMware vSphere 6.0 and VMware Platform Services Controller on a dedicated Cisco UCS C220 M3 or M4 server:
AMP-2P, VMware vSphere 6.0 and Cisco UCS M3 or M4 servers VMware vCenter Server Virtual Appliance server assignments

The following illustration shows the AMP-2P with VMware vSphere 6.0, VMware vCenter Server Virtual Appliance, and VMware Update Manager Database Server on a dedicated Cisco UCS C220 M3 or M4 server:

[Diagram of server assignments]

AMP-2P, VMware vSphere 5.5 and Cisco UCS C220 M4 servers network connectivity

The following illustration shows the network management connectivity for AMP-2P and VMware vSphere 5.5 on Cisco UCS C220 M4 servers:

[Diagram of network connectivity]
AMP-2P, VMware vSphere 5.5 and Cisco UCS M4 servers VMware Single Sign On Service server assignments

The following illustration shows the AMP-2P with VMware vSphere 5.5 and VMware Single Sign On Service on a dedicated Cisco UCS C220 M4 server:
AMP-2P, VMware vSphere 5.5 or 6.0 and Cisco UCS C220 M3 servers network connectivity

The following illustration shows the network management connectivity for AMP-2P and VMware vSphere 5.5 or 6.0 on Cisco UCS C220 M3 servers:

![Network Connectivity Diagram]

AMP-2P, VMware vSphere 5.5 and Cisco UCS M3 servers VM server assignments

**Note:** Converged Systems using VMware Virtual Distributed Switch (VDS) do not include Cisco Nexus1000V VSM VMs.

The following illustration shows the AMP-2P with VMware vSphere 5.5 and VMware Single Sign On Service on a dedicated Cisco UCS C220 M3 server:
Dell EMC VxBlock and Vblock Systems 240 Architecture Overview

Management

Cisco UCS C-Series M3 Server A (Dedicated)
VMware vSphere 5.5 with SSO

* Dual VLAN connectivity
Sample configurations

Sample maximum configuration

Elevations are provided for sample purposes only. For specifications for a specific design, consult your vArchitect.

Rear

- RU 42 AMP Cisco UCS C220 Server
- RU 41 Cisco Nexus 3048 Switch A
- RU 40 Cable management
- RU 39
- RU 38 DAE 0_2
- RU 37
- RU 36 DAE 1_1
- RU 35
- RU 34
- RU 33 DAE 0_1
- RU 32
- RU 31 DAE 1_0
- RU 30
- RU 29 VNX5x00 DME (X-Blades 3 and 2) 0
- RU 28
- RU 27 VNX5x00 control station 1
- RU 26 VNX5x00 control station 0
- RU 25
- RU 24 VNX5x00 DPE: SPB/SPA/DAE 0_0
- RU 23
- RU 22 Reserved for Converged Systems expansion
- RU 21
- RU 20 RecoverPoint Appliance 2
- RU 19 RecoverPoint Appliance 1
- RU 18 Cable management
- RU 17 Cisco UCS C220 Server L
- RU 16 Cisco UCS C220 Server K
- RU 15 Cisco UCS C220 Server J
- RU 14 Cisco UCS C220 Server I
- RU 13 Cisco Nexus 5548UP Switch B
- RU 12
- RU 11 Cable management
- RU 10 Cisco Nexus 5548UP Switch A
- RU 9 Cisco UCS C220 Server H
- RU 8 Cisco UCS C220 Server G
- RU 7 Cisco UCS C220 Server F
- RU 6 Cisco UCS C220 Server E
- RU 5 Cable management
- RU 4 Cisco UCS C220 Server D
- RU 3 Cisco UCS C220 Server C
- RU 2 Cisco UCS C220 Server B
- RU 1 Cisco UCS C220 Server A
Sample minimum configuration

Elevations are provided for sample purposes only. For specifications for a specific design, consult your vArchitect.
## 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</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></td>
<td>virtualization management.</td>
<td></td>
</tr>
<tr>
<td>VMware vSphere ESXi</td>
<td>Virtualizes all application servers and provides VMware High Availability</td>
<td><a href="www.vmware.com/products/vsphere/">www.vmware.com/products/vsphere/</a></td>
</tr>
<tr>
<td></td>
<td>(HA) and Dynamic Resource Scheduling (DRS). (This is available if VMware</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vSphere Enterprise Plus is licensed on all ESXi hosts inside a cluster.)</td>
<td></td>
</tr>
<tr>
<td>VMware Single Sign On (SSO) Service</td>
<td>Provides VMware-specific authentication services.</td>
<td><a href="blogs.vmware.com/kb/2012/10/vsphere-sso-resources.html">blogs.vmware.com/kb/2012/10/vsphere-sso-resources.html</a></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>

## 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>
<tbody>
<tr>
<td></td>
<td>web services, and maintenance data center, branch, and remote office</td>
<td></td>
</tr>
<tr>
<td></td>
<td>applications.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>web services, and maintenance data center, branch, and remote office</td>
<td></td>
</tr>
<tr>
<td></td>
<td>applications.</td>
<td></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 to documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Virtual Distributed Switch (VDS)</td>
<td>A VMware vCenter-managed software switch that delivers advanced network services to virtual machines hosted on that server.</td>
<td><a href="http://www.vmware.com/products/vsphere/features-distributed-switch">http://www.vmware.com/products/vsphere/features-distributed-switch</a></td>
</tr>
</tbody>
</table>

## Storage components

Storage component information and links to documentation are provided.

<table>
<thead>
<tr>
<th>Product</th>
<th>Description</th>
<th>Link to documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>VNX5200 storage array</td>
<td>High-performing unified storage with unsurpassed simplicity and efficiency, optimized for virtual applications.</td>
<td><a href="http://www.emc.com/products/series/vnx-series.htm">www.emc.com/products/series/vnx-series.htm</a></td>
</tr>
</tbody>
</table>