In this section, we will discuss management technologies. As you will learn here, the management technologies used in Dell EMC converged and hyper-converged systems provide significant benefits to our customers.

Click training to navigate directly to the first training topic. Or click assessment to attempt to by-pass the training by taking and passing the assessment for this section.
Recall that Dell EMC Systems are composed of compute, network, storage, virtualization, and management. In the previous sections of this training, you learned about the compute, storage, network, and virtualization. Now you’ll learn about the basics of the Dell EMC System management technology.
Learning Objectives

After completing this module, you will be able to:

- Describe the importance of the management function in a converged infrastructure
- Identify and describe the purpose of element managers and system managers used in Dell EMC Systems
- Identify and describe the purpose of data protection products offered with Dell EMC Systems

The objectives for this section are listed on this page. Upon completion of this training you will be able to describe the importance of the management function in a converged infrastructure. Also, you will be able to identify and describe the purpose of each of the element managers and system managers used in Dell EMC Systems.
Here are the topics that will be addressed in this section. Let’s get started with an introduction to management basics.
We talked earlier about the traditional data center and the amount of work it takes to design, procure, unpack, assemble, test, and implement a new system. However, the larger IT effort comes from trying to make these components continue to work together throughout their lifecycles. Any change to a piece of the infrastructure drives a significant amount of planning, testing, stabilization and optimization. This iterative planning and implementing of updates using manually driven, mistake prone procedures occurs constantly across most infrastructures, with complexity magnified and undue risk raised because organizations are in silos.

Some IT vendors depend upon IT complexity to generate services revenue from customers, rather than trying to eliminate complexity. In summary, most IT staff time and budgets are spent trying to maintain the infrastructure itself, rather than driving innovation.

To transform IT, a new approach is needed.
Dell EMC has pioneered a new way to create converged infrastructure, but equally significant is the way we have pioneered new ways to maintain converged infrastructure.

Among the many things that we do very well at Dell EMC are two things. The first, which we’ve already talk about extensively, is that Dell EMC Systems and our engineering and manufacturing processes enable fast time to deployment. Second, and easier to take for granted is that these systems are engineered to dramatically simplify ongoing customer IT operations.

The tools and processes used to manage and operate systems provide significant IT benefits. Dell EMC System’s strategy and approach to system management are important parts of simplifying ongoing customer IT operations. Now let’s take a closer look at management.
System Management Basic Concepts

At its core, the management infrastructure is designed to manage all the individual components of Dell EMC Systems as well as the systems as a whole. Engineered to facilitate an infrastructure as a service (IaaS) approach to managing and automating the data center with on-demand self-service, resource pooling that speeds implementation of IT services, and measured level of service for monitoring resource use.

The design and function of the management infrastructure itself in Dell EMC converged infrastructures is greatly simplified by virtue of the Advanced Management Platform or AMP. A pre-architected, pre-sized, and pre-configured AMP is deployed to minimize the time and effort needed to architect and size a management environment. You'll learn more about the AMP later.

The point to all this is to create a fully orchestrated management environment with low-touch management to support applications, lifecycle management, and policy driven IT services.
What you will learn here addresses system management on the levels of element managers, system level management, and we will also spend a few minutes talking about data management.

In this training, we can only begin to present some of the tools that comprise the management capabilities that produce the benefits IT departments need. We will feature some important management tools, and provide an overview of how Dell EMC converged and hyper-converged systems are managed.
Now let’s switch gears and talk about element managers.
System Element Managers

Element managers manage individual technology components in Dell EMC systems. These are most often supplied by the manufacture and come with the component.

Think of an element manager this way, if you purchased just a server, or a network switch, or a storage array, you would need to manage that component. Using the element manager provided by the manufacturer you can configure and deploy the component. Perform maintenance and trouble shooting. Or upgrade the tools software or the devices firmware.

Each element manager has at least one interface, and there are three predominant types. Command Line Interface, or CLI. The Graphical User Interface or GUI. And the Application Programming Interface or API.

If you're unfamiliar with these click on the links for more information.
Next, let's take a look at some Cisco compute element managers. Remember that while Vblock Systems will always use Cisco compute components, VxBlock and Dell EMC hyper-converged products may not. So, while we address these Cisco element managers here, be aware that other element managers will be used for non-Cisco servers.

The Cisco Unified Computing System (UCS) Manager is the tool used to manage the compute in systems that utilize Cisco blade servers. It can control multiple servers and/or chassis and can manage resources for thousands of virtual machines. In systems that currently use B-Series Blade Servers and Blade Server chassis, the Cisco UCS Manager is installed on the fabric interconnects where it can manage the compute resources of several blade chassis and the blade servers they contain. A single instance of the Cisco UCS Manager installed on a fabric interconnect can manage up to six fabric interconnects, 24 UCS Server Chassis, and 192 Cisco B-Series Blade Servers.

The element manager used to manage Cisco C-Series rack-mounted servers is very different. Recall that systems with these servers do not contain fabric interconnects and they do not use the Cisco UCS Manager. Instead, management of compute in these systems utilizes the Cisco Integrated Management Controller (CIMC). CIMC, offering both a graphical interface (GUI) and a command line interface (CLI), is installed on every individual server, and each server is managed individually. So, when compute changes are needed across multiple rack mount servers, each CIMC instance is launched and changes administered one C-Series server at a time.

For customers evaluating the purchase of Cisco B-Series blade servers, versus Cisco C-Series rack-mount servers, decisions can come down to the tradeoff of compute management flexibility of the blade technology versus the less costly but more labor-intensive rack-mount alternative.
Element Managers - Network

Tools designed to manage networks and network switches perform tasks like discovering, configuring, and managing network devices. There is one network element manager used for Cisco network switches found in Dell EMC Systems. But remember, like compute element managers, non-Cisco switches will not use these managers.

The network management tool used here is the Cisco Nexus Operating System or NX-OS. It contains both a LAN manager and a SAN manager (which is also referred to as a fabric manager). Cisco NX-OS is found in all Cisco Nexus and Cisco MDS switches. Remember that Cisco Nexus switches can act as a LAN switch or as a Unified switch with both Ethernet ports serving the needs of the LAN network and Fibre channel ports for the SAN network. When a Nexus switch is used as a LAN switch, the NX-OS LAN manager controls the Vblock System LAN. When a Cisco Nexus is used as a Unified switch, the NX-OS LAN manager controls the LAN and the SAN manager controls the SAN. On an MDS SAN switch, the NX-OS SAN manager controls the system SAN. The Cisco NX-OS provides both a command line interface (CLI) or graphical user interface (GUI).
Element Managers - Storage

Element managers used to manage storage arrays are also important to system management. These tools provide an interface to storage arrays for performing storage management tasks such as creating storage device and LUNS, provisioning of virtual storage, managing block level and file level storage, and monitoring performance.

Dell EMC Unisphere is a simple, integrated experience for managing the Dell EMC Unity and VMAX products which are used in Dell EMC converged and hyper-converged systems. With functionality designed for managing both storage and virtualization needs, it’s designed to provide simplicity, flexibility, and automation. Unisphere delivers a common experience with a single interface for managing file and block level storage.
Now that we’re done talking about management on the element or component level, let’s discuss management on the system wide level.
You've learned that Dell EMC systems represent advanced converged and hyper-converged infrastructure technology, which is changing how IT services are managed. There is no doubt these systems are complex engineered products. But the big difference between these and converged products offered by competitors is that Dell EMC engineers this complex technology to not only be easy to purchase and deploy, but also engineered to be easy to maintain.

We do all the hard work of thoroughly testing each component and certifies that all components and their software and firmware are compatible, resulting in a single complete and maintainable configuration. This is a significant benefit to businesses who can avoid the time and resource intensive tasks of monitoring, researching, testing, updating, upgrading and other wise managing each individual component over the system's life cycle.

Remember that Dell EMC converged and hyper-converged infrastructure systems are delivered as a single product, not a bunch of individual IT components. Also, recall that they are deployed as a single product, no assembly required, just plug it in and install production applications and workloads. And finally understand that over the life of the Dell EMC system, it is managed as a single product. Customers don't have to research and plan patches and upgrades to software and firmware on a component-by-component basis. The goal is to eliminate the risks associated with potential operational issues and security vulnerabilities by ensuring only approved configuration options are engaged and that all hardware and software versions are known and approved.
With this in mind, Dell EMC provides to customers a Release Certification Matrix (RCM) for each converged and hyper-converged product. The main purpose of the RCM is to provide a reference of known, approved, and supported configurations of these systems, including hardware, software, and firmware. These are updated on a regular basis when new software and firmware features are added and vulnerabilities are remediated. Using the RCM to update and manage a system results in a consistent, secure, up to date, well tested platform for mission critical workloads over the system's entire life cycle.
The value of the Dell EMC Release Certification Matrix (RCM) for customers is that it takes the guess work out of managing the compatibility of software and firmware releases for every component in Dell EMC converged and hyper-converged systems, as customers upgrade from one RCM release to another. But these save customers an extraordinary amount of time, the IT organization must still identify each component in their system, determine the current state of each components software and firmware, identify which needs to be upgraded, ensure upgrades and patches are compatible across components, download all the upgrades and patches, install each upgrade and patch, and validate the proper installation of each to ensure a healthy system.
Fortunately for customers, not only do they receive RCMs that let them know how to upgrade and maintain the health of their systems, but these systems also come with a tool that makes it extremely easy and time saving to implement and manage the RCM levels.

This tool is Dell EMC Vision Intelligent Operations Software. This software understands the Known Good State (KGS) of Dell EMC converged systems on three levels: optimal system health status, firmware/software release compliance, and security hardening posture.

It provides architecture-aware health monitoring that considers technology component dependencies into system-impact analysis and reporting. At any time customers can view health status of each of their Dell EMC Systems, down to the component level.

Customers can also compare the current state of their system to a more recent Release Certification Matrix, receive a component-by-component report on required updates and upgrades, and also download all needed patches, upgrades, and updates to move their system to a new RCM level.

And finally, using Dell EMC Vision software users can use security hardening profiles to scan their systems for security vulnerabilities. These profiles are based on best practices, component vendor security alerts and software patches, as well as user-customizable policy scans. These scans report on which components present security vulnerabilities and how to mitigate each.

What does all this mean? Well first, customers don't need to know what virtual machine is running on what physical server that maybe failing or is connected to what storage array that may be in an unhealthy state...Dell EMC Vision software does that for them too.
Customers don't need to know what versions of software and firmware is running on what components at what point in time...Dell EMC Vision software does that for them.

Customers don't need to know what configuration settings is needed to harden the security infrastructure of the converged and hyper-converged infrastructure system...Dell EMC Vision software does that for them.

Dell EMC Vision Software provides tools and processes for effectively and efficiently ensuring that converged systems are healthy, optimized, and secure.
VxRack System Management

Management of VxRack systems is a little different, but the same management tasks and functions are addressed. On the physical level, compute, network, and storage components come with their own element managers normally supplied by their manufactures. Like converged infrastructure products, Release Certification Matrices are published for VxRack systems. A special version of Dell EMC Vision software engineered just for VxRack systems is available to manage and automate the process of updating to RCM releases that ensure systems are healthy, optimized, and secure.

In addition, Dell EMC VxRack Manager is available on these systems. This is a unified UI for the management of the entire VxRack System. It provides VxRack System administrators a direct and complete way to deploy, monitor, sustain and support the VxRack System.
The next system management topic in this section, is data protection.
While customer can choose any data protection products and strategy they desire, there are basic capabilities to be concerned about. These include backup and recovery, replication, and business continuity and workload mobility. We'll talk about each of these and about how the Dell EMC Integrated Data Protection offering is an option that addresses each of these.
Once-a-day backups provide minimal required data insurance by protecting against data corruption, accidental data deletion, storage component failure, and site disaster. The daily backup process creates fully recoverable copies of application data.

Daily backups ensure that in a disaster, a business can recover with no more than 24 hours of lost data. The best practice is to replicate the backup data to a second site to protect against a total loss of data in the event of a full site disaster. Most daily backups are saved for 30 to 60 days.

An Integrated Data Protection backup system solution uses a combination of Dell EMC Avamar and Dell EMC Data Domain technology and components. Data Domain systems are used as data storage targets for backups managed and produced by Avamar.
Data Protection - Replication

Daily system backups are important but they don’t capture all critical data. When a system fails or a site disaster occurs, daily backups can be used to recover the data. However, it can only restore data to the state it was in when the last backed up occurred.

For example, if a system stops due to a power failure at 1:37PM on a Thursday, and the last daily backup occurred on Wednesday at 8:00PM, the backup can be used to restore the data to the state it was at 8:00PM Wednesday. But, the daily backup cannot restore the data that was created or changed between 8:00PM Wednesday, when the last backup was completed, and 1:37PM on Thursday.

For data sets that are more valuable, data replication achieves a higher level of data insurance. This creates multiple snapshots of application data throughout the day in between daily backups. In our example, these snapshots are taken every two hours. Snapshots can be used to restore data to a point in time, or to retrieve an individual file. Retrieving a copy of the replicated data reduces the worst-case data loss from 24 hours to the time since the last snapshot was completed.

Dell EMC RecoverPoint is a data replication and recovery product that allows customers to roll back data to potentially any point in time. RecoverPoint is a key component of the Integrated Data Protection product family, enhancing operational recovery, disaster recovery processes, and reducing potential data loss.

RecoverPoint is typically deployed to protect specific business applications and data that need more data protection than a once-per-day backup provides.
Business continuity and workload mobility go even further. Business continuity ensures zero data loss and near-zero recovery time for business-critical data. Business continuity protection ensures that no data is lost in the event of a system failure or site disaster. And not only is data immediately safe, it is nearly immediately available to launch on another system.

While business continuity helps IT respond to unexpected events, workload mobility provides ability to proactively protect data by moving applications and data to another site in anticipation of a problem. For example, when a data center is in the path of a threatening storm, critical applications and their data can be moved to a data center out of the storm’s path. This requires a good workload mobility strategy, which easily and with zero down time can move applications and data to a safe environment. Workload mobility is also great for moving applications and data to balance workloads across systems.

Dell EMC VPLEX enables business continuity, dynamic workload mobility and continuous availability within and between systems no matter what the distance. A VPLEX cluster is located in the data path between the system servers and storage to create data copies. Copies can be created and stored locally or over a distance. It provides simultaneous access to storage devices at two sites through the creation of data copies. These are created as VPLEX distributed virtual volumes, which is supported at each site by a VPLEX cluster. This capability contributes to a business’ ability to ensure zero data loss and near-zero recovery time for business-critical data.
In the final topic of this section, we’ll address the Advanced Management Platform or AMP. This system management function is found in Dell EMC converged infrastructure systems. Click next to learn more.
Advanced Management Platform (AMP)

The Advanced Management Platform (AMP) is a management system that resides in Dell EMC converged infrastructure systems, but is distinct and separate from components that run clients' business production workloads. It is comprised of hardware and software to run management applications and tools used to monitor and manage the system's health, performance, and capacity.

For hardware is includes one to three Cisco C-Series rack mount servers, two Cisco Nexus network switches, and an EMX VNXe storage array. Depending on the system and the client's system management strategy, there are a number of configurations available.
Sizing of the AMP is partially determined by the software and applications loaded on it. With Dell EMC converged infrastructure products, there are core management workloads, and optional management workloads.

The Core Management Workload is the minimum set of required management software needed to install, operate, and support a converged infrastructure system. This includes all hypervisor management tools, element managers, virtual networking components (Cisco Nexus 1000V or VMware VDS), and Dell EMC Vision Intelligent Operations software.

The Optional Management Workload is non-Core Management Workloads. The primary purpose of these is to manage components within a converged infrastructure systems. The list includes but is not limited to Data Protection solutions, security software, or storage management tools such as Avamar Administrator and others.