



Technical Report

FlexPod Security Hardening

Jyh-shing Chen, NetApp
September 2025 | TR-4984-0925

In partnership with



Abstract

This technical report includes an introduction to FlexPod[®] solutions and offers guidance and configuration examples at the compute, network, storage, and virtualization layers to harden FlexPod solution security to help organizations achieve their security objectives.

TABLE OF CONTENTS

<i>FlexPod Security Hardening</i>	1
<i>FlexPod introduction</i>	6
FlexPod overview	6
FlexPod benefits	7
FlexPod components	7
Cisco compute components	7
Cisco switching components	10
NetApp storage components	12
FlexPod topologies	13
Single-site solutions.....	13
Multi-site solutions	16
<i>FlexPod security hardening</i>	18
Validation topology	19
Hardware and software	19
General considerations	20
Management plane, control plane, and data plane.....	20
Bastion Host	21
Internet proxy server.....	21
Disable unused services.....	21
Use secure protocols	21
Network and traffic segmentation	21
VLANs.....	21
VMware virtual networking.....	23
ONTAP IPspaces.....	24
Network access restriction	24
Cisco Nexus IP ACL configuration.....	24
Login authentication	25
Password strengths and policies	25
Lightweight Directory Access Protocol authentication	25
Cisco UCS Manager login authentication	25
Cisco Nexus login authentication.....	26
NetApp ONTAP login authentication	28
VMware vSphere login account and authentication.....	33
Role-based access control	34
Cisco UCS Manager role-based access control	34
Cisco Nexus role-based access control.....	36
NetApp ONTAP role-based access control	37
VMware vSphere role-based access control	39
Login banners	40
Cisco UCS Manager login banners	40
Cisco Nexus login banners	43
NetApp ONTAP login banners.....	43

VMware vSphere login banners.....	44
Login session timeout and limits	49
Cisco UCS Manager login session timeout and limits	49
Cisco Nexus login session timeout and limits.....	51
NetApp ONTAP login session timeout and limits.....	51
VMware vSphere login session timeout and limits	52
Time synchronization	54
Cisco UCS Manager time synchronization	54
Cisco Nexus time synchronization.....	55
NetApp ONTAP time synchronization.....	56
VMware vSphere time synchronization	57
Remote logging	58
Cisco UCS Manager remote logging	58
Cisco Nexus remote logging.....	59
NetApp ONTAP remote logging.....	60
VMware vSphere remote logging	63
Configuration backup	66
Cisco UCS Manager configuration backup.....	66
Cisco Nexus configuration backup	68
NetApp ONTAP configuration backup	71
VMware vCenter Sever backup.....	72
FIPS 140 compliance	73
Cisco UCS FIPS 140 compliance	73
Cisco Nexus FIPS 140 compliance	73
NetApp ONTAP FIPS 140 compliance	75
VMware vSphere FIPS 140 compliance.....	76
UEFI secure boot.....	80
Cisco UCS Manager secure boot	80
VMware vCenter Server secure boot attestation.....	81
VMware ESXi secure boot.....	82
NFS access authorization	83
Layered access configuration overview	83
ONTAP export policy	84
Mount NFS volume in VMware	84
Kerberos considerations	85
ONTAP data-at-rest encryption.....	86
ONTAP data-in-flight encryption.....	86
ONTAP IPsec data-in-flight encryption	86
ONTAP cluster peering encryption	87
ONTAP ransomware protection	88
FPolicy	88
Volume Snapshot and policy	89
Autonomous ransomware protection	90
SnapLock protection / compliance.....	91
Support information.....	91
Cisco UCS Call Home	91
Cisco Nexus Smart Call Home	92
NetApp ONTAP support information.....	92
VMware support information.....	93

Security advisories	95
Cisco security advisories	95
Cisco Intersight security advisories	98
NetApp security advisories	100
VMware security advisories	101
Image validation	103
Cisco UCS Manager image validation	104
Cisco Nexus image validation.....	104
NetApp image validation.....	105
VMware image validation.....	106
Conclusion	107
Appendix A: UEFI secure boot service profile move	108
Prepare for service profile move	108
Update server pool	109
Resolve service profile boot issue	111
Resolve the vCenter Server reported TPM issues	114
Appendix B: ONTAP multi-admin verification example.....	117
Add additional administrators	118
Create an administrator approval group	118
Enable multi-admin verification.....	118
Add multi-admin verification rule.....	119
Initiate a protected operation	120
Approve a protected operation	120
Complete a protected operation	120
Exercising the newly protected volume delete operation.....	121
Where to find additional information.....	123
Version history	127

LIST OF TABLES

Table 1) NetApp AFF / ASA / FAS product family systems technical documentation.	13
Table 2) Hardware and software used for solution validation.	20
Table 3) Configured VLANs and their usage.	22
Table 4) Example predefined user roles for Cisco UCS Manager software.	34
Table 5) Example user privileges for Cisco UCS Manager software.	35
Table 6) Example predefined user roles for Cisco NX-OS software.	36
Table 7) Example predefined roles for ONTAP cluster administrators.	37
Table 8) Predefined roles for ONTAP SVM administrators.	38
Table 9) Predefined vCenter Server roles and description.	39
Table 10) vCenter Server local user roles and capabilities.	40
Table 11) Supported host key type algorithms for ONTAP SSH connections.	75

LIST OF FIGURES

Figure 1) FlexPod solution components.	6
Figure 2) Cisco UCS C-Series rack servers, UCS 5108 chassis with B-Series blades, and UCS X9508 chassis with X-Series compute nodes.	8
Figure 3) Cisco UCS fabric extenders for the UCS 5108 chassis and UCSX intelligent fabric module for the 9508 chassis.	8
Figure 4) Cisco UCS 5 th , 4 th , and 3 rd generation Fabric Interconnects.	9
Figure 5) Cisco UCS VICs for B-Series / C-Series servers and X-Series compute nodes.	10
Figure 6) Example Cisco Nexus 9K and 3K switches.	11
Figure 7) Example Cisco MDS 9100 / 9200 / 9300 Series switches.	11
Figure 8) Example NetApp storage controllers and disk shelves.	13
Figure 9) Simple FlexPod solution topology with minimum resource requirements.	14
Figure 10) FlexPod solution topology with UCS Mini and UCS C-series.	15
Figure 11) FlexPod solution topology with UCS X-series chassis and compute nodes.	15
Figure 12) FlexPod MetroCluster IP solution topology with ONTAP Mediator deployed at a third site.	16
Figure 13) FlexPod SM-BC solution components.	17
Figure 14) FlexPod SM-BC solution topology deployed with a multi-site fabric.	17
Figure 15) FlexPod SM-BC solution topology for a datacenter with multiple branch offices.	18
Figure 16) FlexPod solution validation component-level topology.	19
Figure 17) UCS Manager VLAN configurations.	22
Figure 18) Virtual networking vNICs, vSwitchs, and vDS.	23

FlexPod introduction

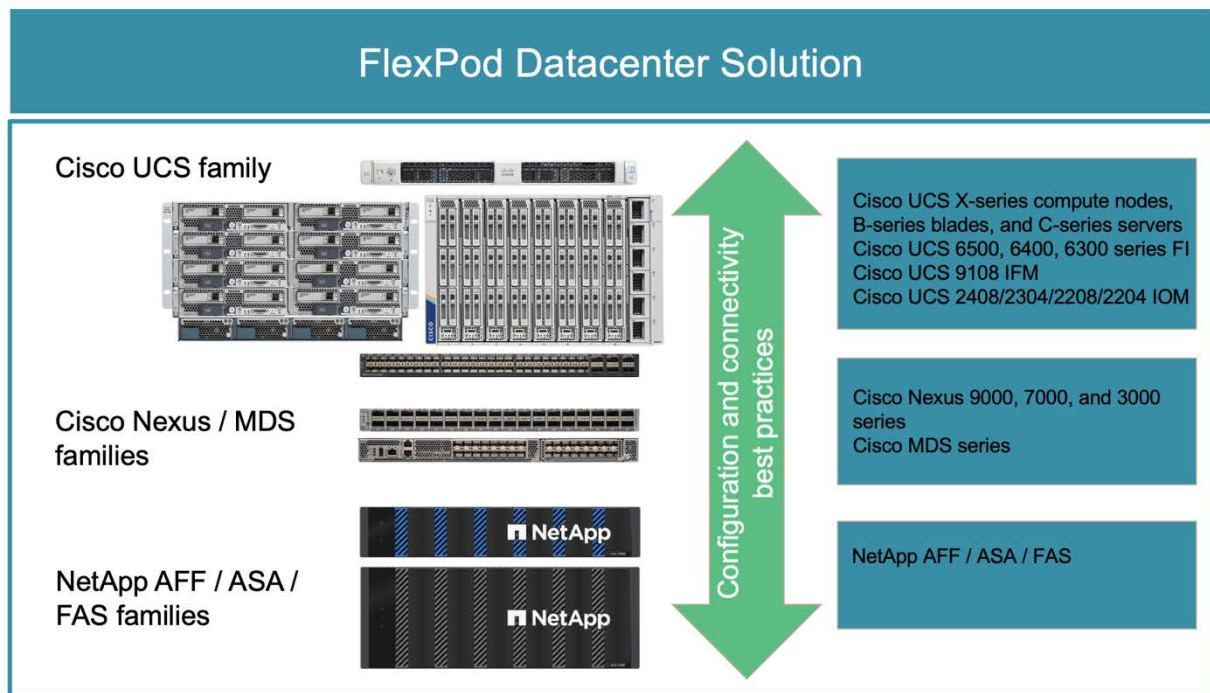
FlexPod overview

FlexPod® is a best practice converged infrastructure data center architecture that includes the following components from Cisco® and NetApp®:

- Cisco Unified Computing System (Cisco UCS)
- Cisco Nexus and MDS families of switches
- NetApp Fabric Attached Storage (FAS), All Flash FAS (AFF), and All SAN Array (ASA) systems

Shown in Figure 1 are some of the components utilized for creating FlexPod solutions. These components are connected and configured according to the best practices of both Cisco and NetApp to provide an ideal platform for running a variety of enterprise workloads with confidence.

Figure 1) FlexPod solution components.



A large portfolio of Cisco Validated Designs (CVDs) and NetApp Verified Architectures (NVAs) are available. These CVDs and NVAs cover all major data center workloads and are the results of continued collaborations and innovations of NetApp and Cisco on FlexPod solutions.

Incorporating extensive testing and validations in their creation process, FlexPod CVDs and NVAs provide reference solution architecture designs and step-by-step deployment guides to help partners and customers deploy and adopt FlexPod solutions. By using these CVDs and NVAs as guides for design and implementation, businesses can reduce risks, reduce solution downtime, and increase the availability, scalability, flexibility, and security of the FlexPod solutions they deploy.

Each of the FlexPod component families shown (Cisco UCS, Cisco Nexus/MDS switches, and NetApp storage) offers platform and resource options to scale the infrastructure up or down, while supporting the features and functionalities that are required under the configuration and connectivity best practices of FlexPod. FlexPod can also scale out for environments that require multiple consistent deployments by rolling out additional FlexPod stacks.

FlexPod benefits

The FlexPod Datacenter solution offers the following key customer benefits:

- Highly available design across all infrastructure layers with no single point of failure.
- Scalable design with the flexibility to add compute capacity, storage performance and capacity, or network bandwidth as needed.
- Hybrid-cloud ready and policy-driven modular design that can be replicated to expand and grow as the needs of the business grow.
- Flexible design that can support components beyond what is validated and documented by utilizing configurations supported by Cisco and NetApp interoperability matrixes.
- Support for component monitoring, solution automation and orchestration, and workload optimization.
- Cooperative support model and Cisco Solution Support.

FlexPod components

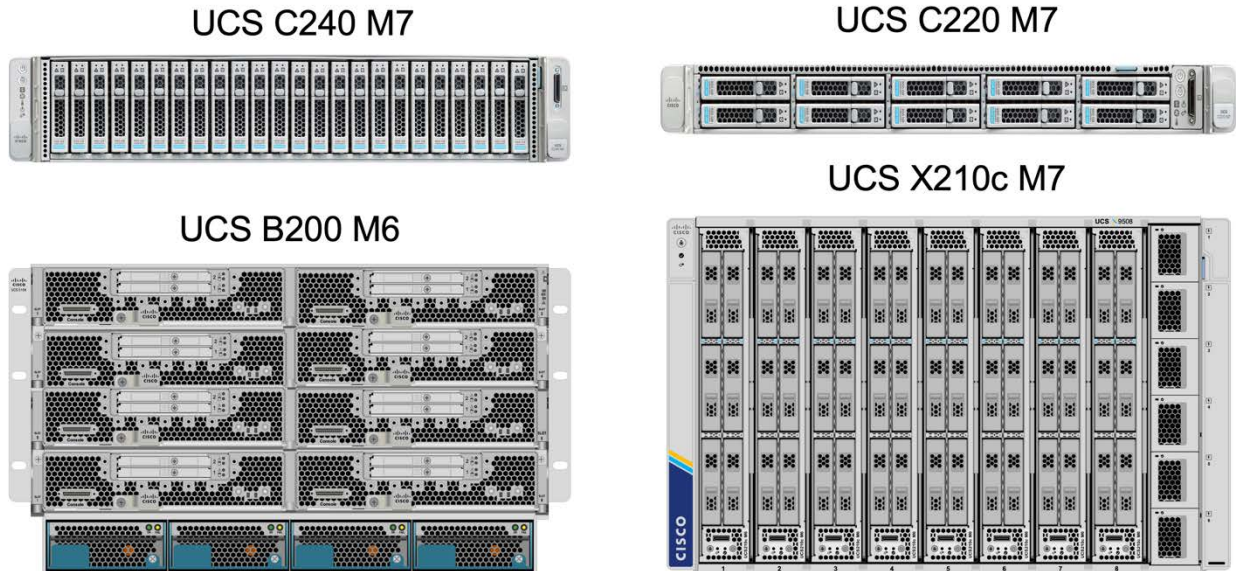
Cisco compute components

The Cisco Unified Computing System (UCS) is an integrated computing infrastructure to provide unified computing resources, unified fabric, and unified management. It enables companies to automate and accelerate deployment of applications, including virtualization and bare-metal workloads. The Cisco UCS supports a wide range of deployment use cases including remote and branch locations, data centers, and hybrid cloud use cases. Depending on the specific solution requirements, the FlexPod implementation can utilize a variety of Cisco compute components and at different scales. The following subsections provide additional information on some of the UCS components.

UCS server / compute node

Shown in Figure 2 are some examples of the UCS server components, including UCS C-Series rack servers, UCS 5108 chassis with B-Series blade servers, and the new UCS X9508 chassis with X-Series compute nodes. The Cisco UCS C-Series rack servers are available in one and two rack-unit (RU) form factor, Intel and AMD CPU based models, and with various CPU speed/cores, memory, and I/O options. The Cisco UCS B-Series blade servers and the new X-Series compute nodes are also available with various CPU, memory, and I/O options and they are all supported in the FlexPod architecture to meet the diverse business requirements.

Figure 2) Cisco UCS C-Series rack servers, UCS 5108 chassis with B-Series blades, and UCS X9508 chassis with X-Series compute nodes.



In addition to the latest generation C220 / C240 M7 rack servers, B200 M6 blade servers, and X210c M7 compute nodes shown in the figure, prior generation rack and blade server variants can also be utilized while they are still supported.

IO Module and Intelligent Fabric Module

I/O Module (IOM) / Fabric Extender and Intelligent Fabric Module (IFM) provide unified fabric connectivity for the Cisco UCS 5108 blade server chassis and the Cisco UCS X9508 X-Series chassis, respectively.

The fourth generation UCS IOM 2408 has eight 25-G unified Ethernet ports for connecting the UCS 5108 chassis with Fabric Interconnect (FI). Each 2408 has four 10-G backplane Ethernet connectivity through the midplane to each blade server in the chassis.

The UCSX 9108 100G IFM has eight 100-G unified Ethernet ports for connecting the blade servers in the UCS X9508 chassis with FIs. Each 9108 has one 100-G connection, or four 25-G lanes (depending on the VIC installed in the server), towards each UCS X210c compute node in the X9108 chassis. The 9108 IFM also works in concert with the FI to manage the chassis environment.

Shown in Figure 3 are the UCS 2304 and 2408 IOMs for the UCS 5108 chassis and the 9108 IFM for the X9508 chassis.

Figure 3) Cisco UCS fabric extenders for the UCS 5108 chassis and UCSX intelligent fabric module for the 9508 chassis.

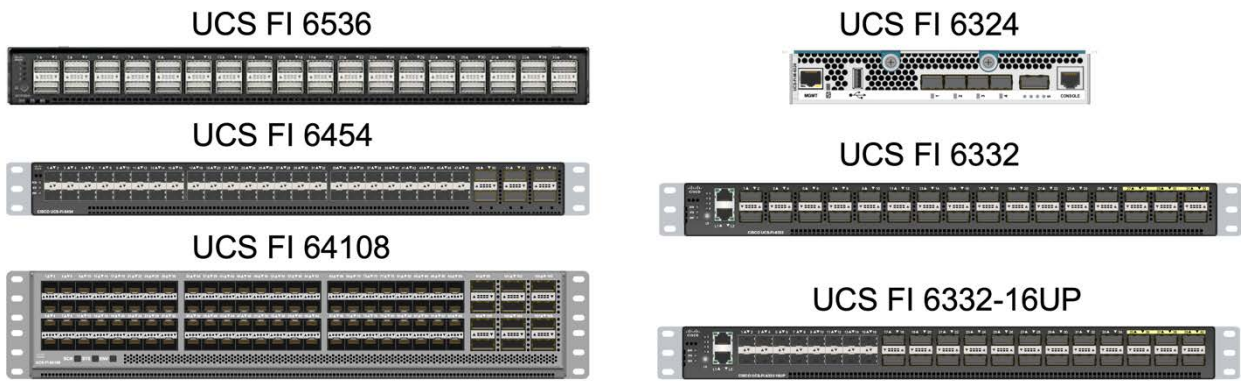


UCS Fabric Interconnects

The Cisco UCS Fabric Interconnects (FIs) provide connectivity and management for the entire Cisco UCS. Typically deployed as an active/active pair, the system's FIs integrate all components into a single, highly available management domain controlled by the Cisco UCS Manager or Cisco Intersight. Cisco UCS FIs provide a single unified fabric for the system, with low-latency, lossless, cut-through switching that supports LAN, SAN, and management traffic using a single set of cables.

The latest 5th generation Cisco UCS FI 6536 supports 100/40/25/10 Gbps Ethernet ports and 32Gbps Fibre Channel ports using breakout cables. There are two variants for the 4th generation Cisco UCS FIs, UCS FI 6454 and 64108. They include support for 10/25 Gbps Ethernet ports, 1/10/25-Gbps Ethernet ports, 40/100-Gbps Ethernet up-link ports, and unified ports that can support 10/25 Gigabit Ethernet or 8/16/32-Gbps Fibre Channel. Figure 4 shows the 5th and 4th generation Cisco UCS FIs along with the 3rd generation models which are also supported.

Figure 4) Cisco UCS 5th, 4th, and 3rd generation Fabric Interconnects.



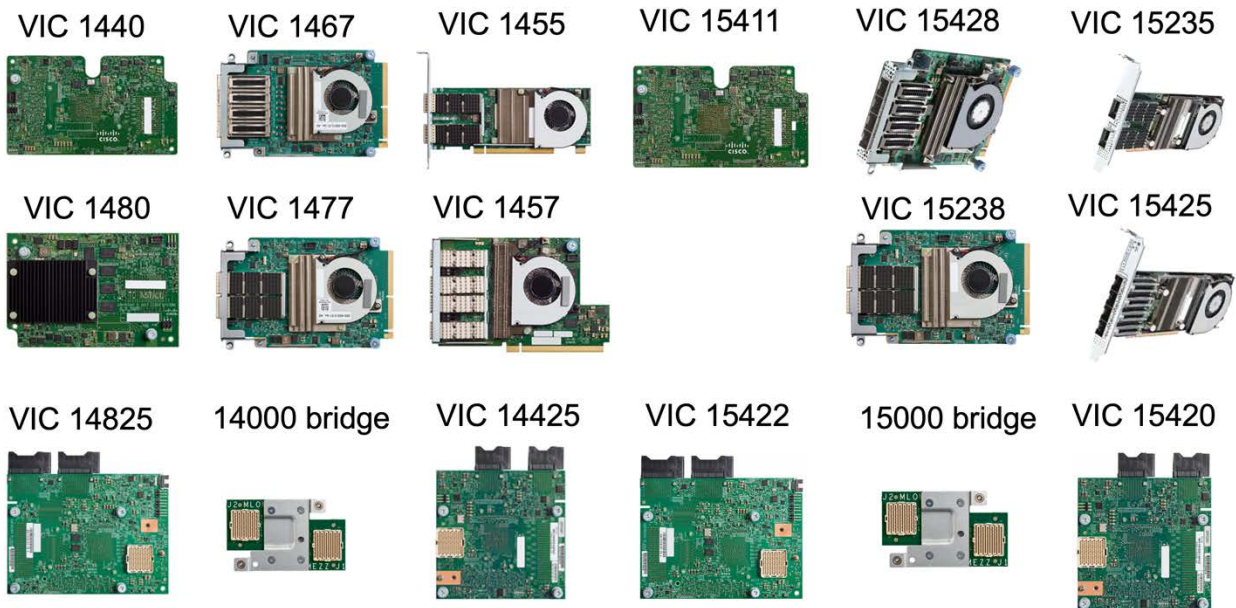
Note: While the Cisco UCS X-Series chassis with 5th or 4th generation fabric interconnects were initially supported in Intersight Managed Mode (IMM) only, the UCS Manager 4.3 release supports the X-Series chassis and compute nodes in UCSM mode. The Cisco UCS 5108 B-series chassis can be supported both in IMM mode and in UCSM managed mode also.

Note: The UCS FI 6324 uses IOM form factor and is embedded in a UCS Mini chassis for deployments which require only a small UCS domain.

UCS Virtual Interface Cards

Cisco UCS Virtual Interface Cards (VICs) unify system management, LAN, and SAN connectivity for rack and blade servers. It supports up to 512 virtual devices, either as virtual Network Interface Cards (vNICs) or as virtual Host Bus Adapters (vHBAs) using the Cisco SingleConnect technology. As a result of virtualization, the VIC cards greatly simplify the network connectivity and reduces the number of network adapters, cables, and switch ports needed for solution deployment. Shown in Figure 5 are some of the Cisco UCS VICs available for the B-Series / C-Series servers and the X-Series compute nodes.

Figure 5) Cisco UCS VICs for B-Series / C-Series servers and X-Series compute nodes.



The different adapter models support different blade and rack servers with a variety of port count, port speed, and form factors of modular LAN on Motherboard (mLOM), mezzanine card, and PCIe interface. The adapters can support some combinations of 10/25/40/100/200-G Ethernet and Fibre Channel over Ethernet (FCoE). They incorporate Cisco's Converged Network Adapter (CNA) technology and support a comprehensive feature set and simplify adapter management and application deployment. With a combination of Cisco VIC in mLOM, mezzanine, and port expander / bridge card configurations, you can fully take advantage of the bandwidth and connectivity available to the blade servers.

For details on the Cisco UCS product families, technical specifications, and documentation, please refer to the [Cisco UCS](https://www.cisco.com/c/en/us/products/universalcisco-ucsb.html) web site for information.

Cisco switching components

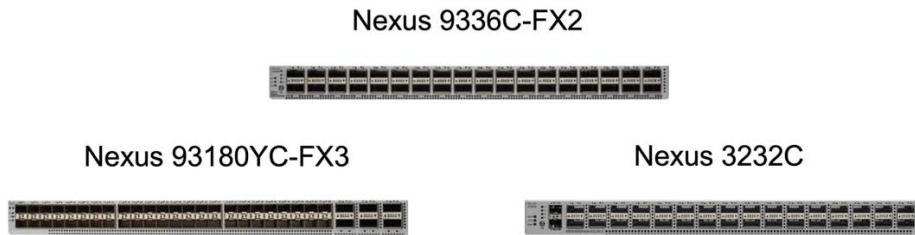
Nexus switches

FlexPod utilizes Cisco Nexus Series switches to provide Ethernet switching fabric for communications between the Cisco UCS and NetApp storage controllers. All currently supported Cisco Nexus switch models, including the Cisco Nexus 3000, 7000, and 9000 Series, are supported for FlexPod deployment.

When selecting a switch model for FlexPod deployment, there are many factors to consider, such as performance, port speed, port density, switching latency, and technology such as ACI and VXLAN support, for your design objectives as well as the switches' support timespan.

The validation for many recent FlexPod CVDs utilizes the Cisco Nexus 9000 series switches, such as the Nexus 9336C-FX2 and the Nexus 93180YC-FX3, which deliver high performance 10/25/40/100G ports, low latency, and exceptional power efficiency in a compact 1U form factor. Figure 6 shows a few Cisco Nexus 9k and 3k switches, including the Nexus 9336C-FX2 and the Nexus 3232C utilized for this validation.

Figure 6) Example Cisco Nexus 9K and 3K switches.

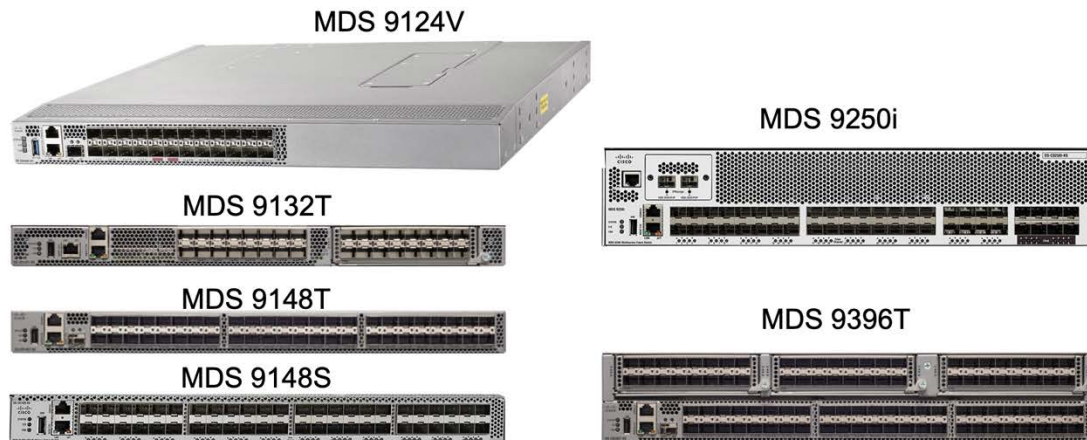


Please refer to [Cisco Data Center Switches](#) for more information on the available Nexus switches and their specifications and documentation.

MDS switches

The Cisco MDS 9000 Series Fabric switches are an optional component in the FlexPod architecture. These switches are highly reliable, highly flexible, secure, and can provide visibility into the traffic flow in the fabric. Figure 7 shows some example fixed MDS switches that can be utilized to build redundant FC SAN fabrics for a FlexPod solution to meet application and business requirements.

Figure 7) Example Cisco MDS 9100 / 9200 / 9300 Series switches.



The Cisco MDS 9132T / 9148T / 9396T high performance 32G Multilayer Fabric Switches are cost effective and are highly reliable, highly flexible, and highly scalable. The next-generation Cisco MDS 9124V 64 Gbps 24-port Fibre Channel switch supports 64, 32, and 16 Gbps FC ports for high-speed connectivity for all-flash arrays and high-performance hosts. The advanced storage networking features and functions come with ease of management and are compatible with the entire Cisco MDS 9000 family portfolio for a reliable SAN implementation.

The state-of-the-art SAN analytics and telemetry capabilities are built into these next-generation hardware platform. The telemetry data extracted from the inspection of the frame headers can be streamed to an analytics-visualization platform, including the Cisco Data Center Network Manager. The MDS switches supporting 16G FC, such as the MDS 9148S, are also supported in FlexPod. In addition, Multiservice MDS switches, such as MDS 9250i which supports FCoE and FCIP protocols in addition to FC protocol, are also part of the FlexPod solution portfolio.

On the semi-modular MDS switches such as 9132T and 9396T, additional port expansion module and port license can be added to support additional device connectivity. On the fixed switches such as 9148T, additional port licenses can be added as needed. These pay-as-you-grow flexibility provide an operational

expenses component to help reduce the capital expenses for the implementation and operation of the MDS switches-based SAN infrastructure.

Please refer to [Cisco MDS Fabric Switches](#) for more information on the available MDS Fabric switches and see the [NetApp IMT](#) and [Cisco Hardware and Software Compatibility List](#) for a complete list of supported SAN switches.

NetApp storage components

Redundant NetApp Fabric Attached Storage (FAS), All Flash FAS (AFF), or All SAN Array (ASA) storage systems running the latest ONTAP® software releases are recommended for creating FlexPod solutions. Running the latest ONTAP release allows you to take advantages of the continued ONTAP innovations, performance and quality improvements, and bug fixes and security vulnerability patches.

NetApp storage systems provide a hybrid cloud foundation for customers to take advantage of the seamless data mobility enabled by NetApp Data Fabric. With NetApp Data Fabric, you can easily get data from the edge where it is generated to the core where it is utilized and to the cloud to take advantage of the on-demand elastic compute and AI / ML capabilities to gain actionable business insights from your valuable data.

NetApp FAS storage systems (FAS 2720 / 2750 / 2820 / 8300 / 8700 / 9500) are powered by NetApp ONTAP data management software to help you build a storage infrastructure that is simple, secure, and trusted. NetApp FAS storage systems provide customers with a balance of performance and capacity. Optimized for easy deployment and operations, NetApp FAS storage systems deliver the flexibility to handle your future growth and cloud integration. With highly available hardware and powerful software, FAS storage systems cost-effectively deliver the data protection, security, and scalability to safeguard your data and drive efficient operations.

NetApp AFF A-Series and ASA A-Series storage systems (AFF A150 / A250 / A400 / A800 / A900, ASA A150 / A250 / A400 / A800 / A900) with industry leading performance and innovations provide enterprise data protection and feature-rich data management capabilities. The AFF A-Series and ASA A-Series systems support end-to-end NVMe technologies, including NVMe-attached SSDs, NVMe over FC (NVMe/FC), and NVMe over TCP (NVMe/TCP), and FC and iSCSI front-end host connectivity. If you already have an existing FlexPod deployment using an FC infrastructure that can support NVMe/FC, you can adopt NVMe/FC protocol to improve your workload throughput and reduce IO latency without infrastructure changes.

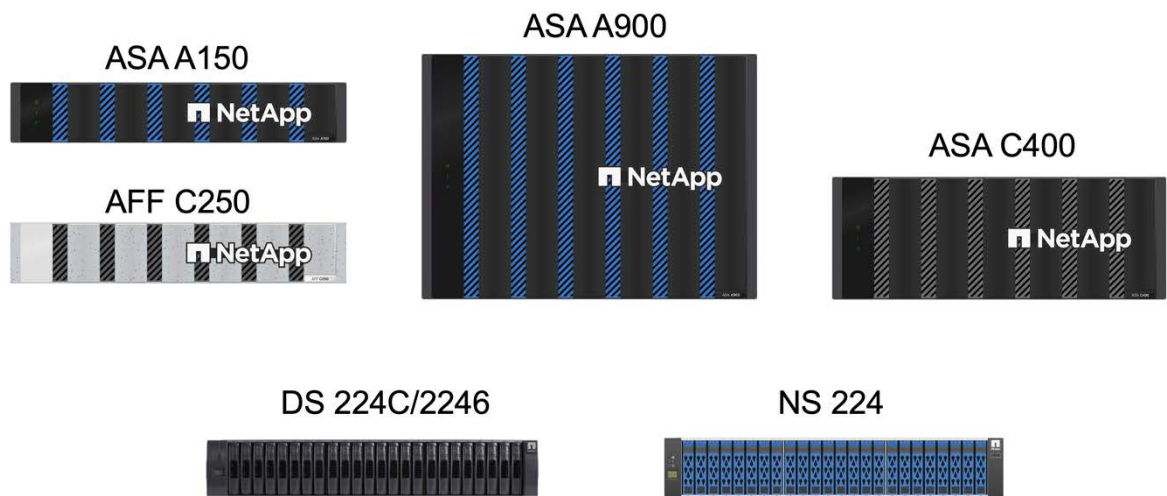
NetApp AFF C-Series and ASA C-Series storage systems (AFF C250 / C400 / C800, ASA C250 / C400 / C800) help move more data to flash with the latest high-density NVMe QLC capacity flash technology. These systems are suited for capacity-intensive workloads such as tier-2 databases, general purpose virtualization, and backup and recovery that don't require sub-millisecond latency. The large-capacity, small-footprint deployment is an affordable way to modernize data center to all flash and connect to cloud. Powered by NetApp ONTAP data management software, NetApp AFF C-Series and ASA C-Series systems deliver industry-leading efficiency, superior flexibility, and best-in-class data services and cloud integration to help scale IT infrastructure, simplify data management, reduce storage cost, rack space usage, power consumption, and improve sustainability significantly.

NetApp ASA A-Series and NetApp ASA C-Series storage systems extend the ONTAP experience to provide all-flash, SAN-optimized storage systems to accelerate and modernize the data infrastructure. Powered by symmetric active-active architecture, these ASA systems keep your data secure with six nines (99.9999%) availability guarantee so you can deploy your mission-critical workloads on them with peace of mind.

NetApp offers a variety of storage systems and disk shelves to meet your performance and capacity requirements. NetApp storage systems and NetApp Ransomware Recovery Guarantee offers a cost-effective approach to cyber resilience with more protection and security. Please see Figure 8 for some example systems from the NetApp storage system portfolio. Please see Table 1 for links to product

pages for detailed information about NetApp AFF, ASA, and FAS storage systems' capabilities and specifications.

Figure 8) Example NetApp storage controllers and disk shelves.



Note: The above picture only shows a small subset of the available NetApp storage controllers. For example, in addition to the AFF C250 shown above, there are also AFF A250, ASA A250, and ASA C250 models that share the same form factor as the AFF C250 but have different front bezels and performance / capacity characteristics.

Table 1) NetApp AFF / ASA / FAS product family systems technical documentation.

Product family	Technical documentation
AFF A-series systems	AFF A-series documentation
AFF C-series systems	AFF C-series documentation
ASA A-series systems	ASA A-series documentation
ASA C-series systems	ASA C-series documentation
FAS systems	FAS systems documentation

Please consult the [NetApp disk shelves and storage media documentation](#) and [NetApp Hardware Universe](#) for details on the disk shelves and the supported disk shelves for each storage controller model,

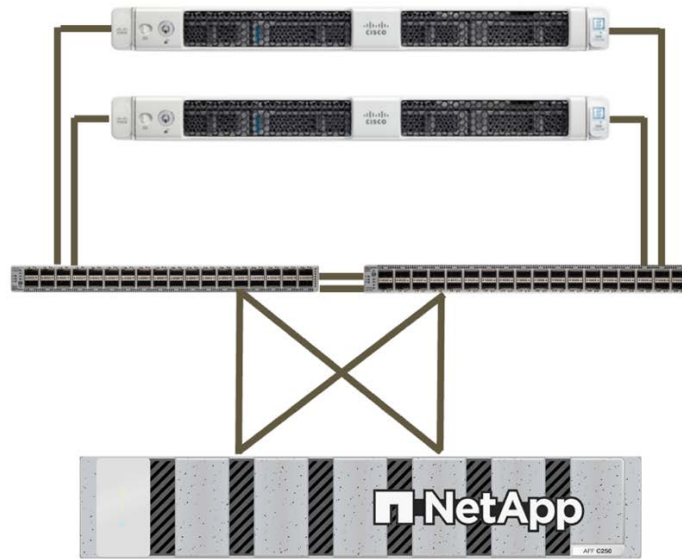
FlexPod topologies

FlexPod solutions are flexible in configuration. A reference FlexPod configuration from a Cisco Validated Design (CVD) or NetApp Verified Architecture (NVA) can be scaled up, scaled down, or scaled out to meet different solution requirements.

Single-site solutions

For a FlexPod solution which requires only minimum compute and storage resources, it can take a very simple solution topology as illustrated in Figure 9.

Figure 9) Simple FlexPod solution topology with minimum resource requirements.



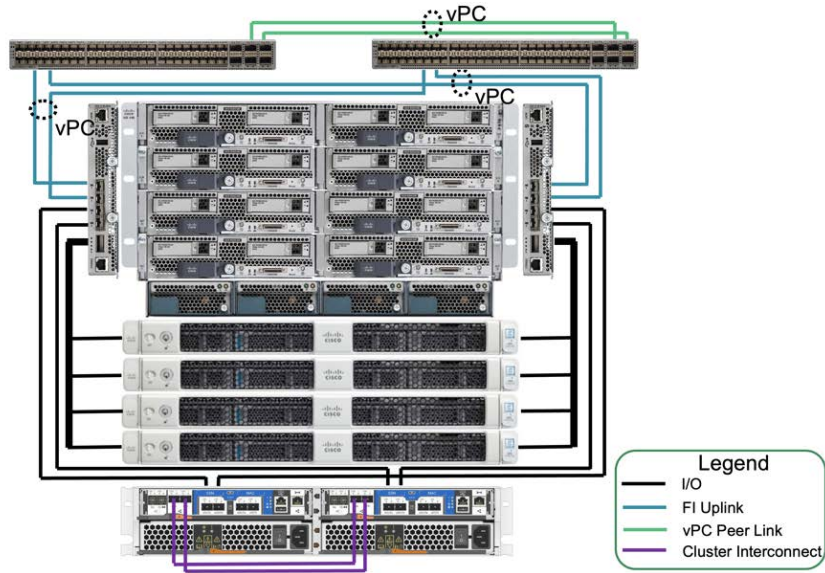
This simple topology uses two Cisco UCS C-Series rack servers, two Cisco Nexus switches, and one highly available NetApp AFF / ASA / FAS storage controller pair with the internal disk shelf.

As your business grows and more resources are required from your solution, you can grow your FlexPod in various ways at the compute, network, and storage layers. For example, you might add or upgrade to provide additional CPU and memory resources, add additional servers, increase network bandwidth with additional connectivity, and provide additional storage capacity or I/O performance by adding storage shelves and additional storage controllers.

There are alternatives to utilizing the Cisco UCS C-series rack servers for a small scale FlexPod deployment. For example, the Cisco UCS Mini configuration can accommodate up to eight servers in a single chassis. With its embedded fabric interconnect, UCS FI 6324, UCS Mini simplifies server management and external network connectivity.

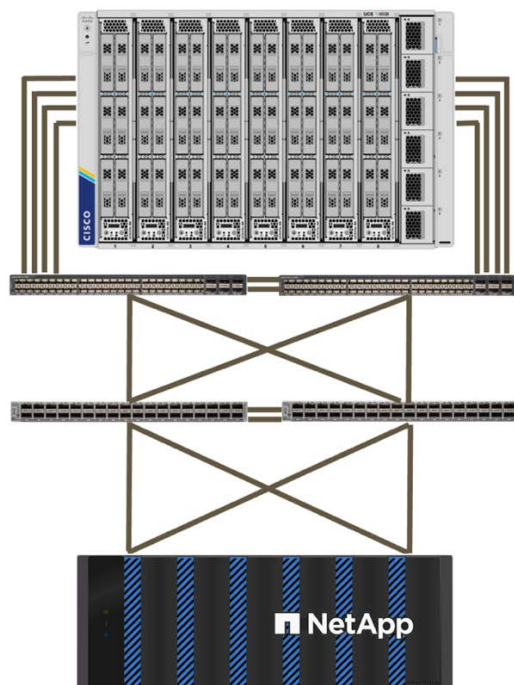
The UCS Manager running on the FI provides service profiles for consistent policy-based server deployment configurations. In addition, you can easily replace a server and have the new server take over the identity and configurations of the replaced server. With growth in mind, you can start with just two servers and grow to eight servers as needed without any additional cabling. Up to four external UCS C-series rack servers can be connected to the embedded UCS FI 6324 to simplify server management as shown in Figure 10.

Figure 10) FlexPod solution topology with UCS Mini and UCS C-series.



To meet the workload requirements of a data center, more compute and storage resources are needed in addition to higher performance. A FlexPod solution architecture for data center deployment might look like Figure 11. The Cisco UCS X-series chassis and compute nodes provide unparalleled performance and scalability. The fabric interconnects can be configured to operate in Cisco Intersight Managed Mode (IMM) or Cisco UCS Manager Managed Mode (UCSM), depending on your preference. The server profile in IMM mode and service profile in UCSM mode provide similar policy-based management for easy server deployments. The mid-range and high-end NetApp AFF and ASA storage controllers can be selected to provide the right storage performance and capacity to meet the requirements of mission-critical workloads.

Figure 11) FlexPod solution topology with UCS X-series chassis and compute nodes.



Multi-site solutions

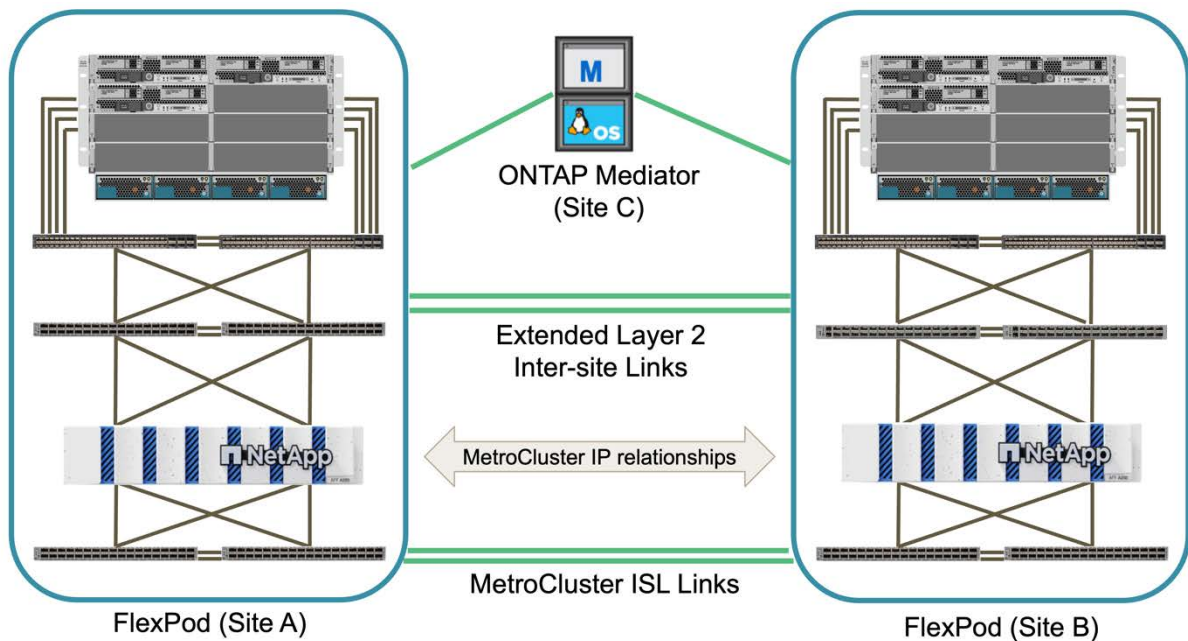
FlexPod solutions use redundant compute, network, and storage components that are interconnected with redundant connectivity. This highly available design approach provides solution resiliency and enables the solution to withstand single-point-of-failure scenarios.

A multi-site solution design with two FlexPods and ONTAP MetroCluster™ IP or ONTAP SnapMirror® Business Continuity (SM-BC) solution can take data protection to the next level. These multi-site FlexPod solutions implement synchronous data replication across sites to ensure that business-critical data services are available despite a potential single-site failure.

FlexPod MetroCluster IP solution deployments typically utilize identical storage controller hardware configurations for the two sites. With FlexPod MetroCluster IP solution, you can create an active-active multi-site data center. Both NAS and SAN workloads can be served from the AFF storage systems deployed at both sites of the solution and workloads can be switched over to the other site for disaster recovery testing, site maintenance, or actual site failure scenarios.

Figure 12 illustrates a FlexPod MetroCluster IP solution where the two FlexPods can be deployed at sites up to 700 Kms apart. The solution synchronously replicates data between sites to achieve zero recovery point objective (RPO) and very low recovery time objectives (RTO). The ONTAP Mediator deployed at a third site monitors the solution and facilitates automatic switchover when a site disaster is detected.

Figure 12) FlexPod MetroCluster IP solution topology with ONTAP Mediator deployed at a third site.

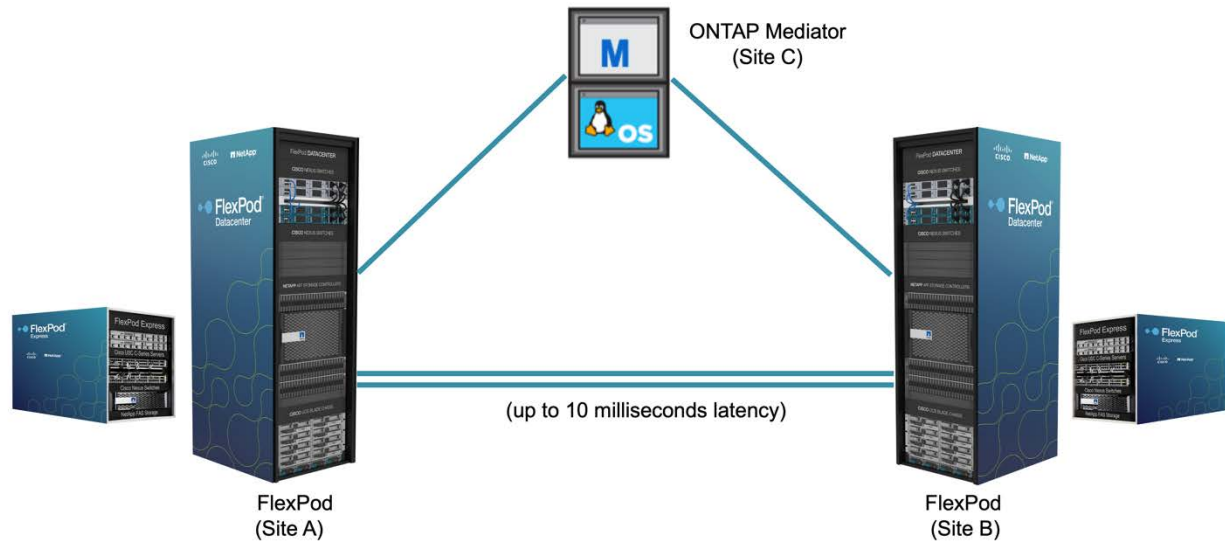


On the other hand, FlexPod SM-BC solutions, which synchronously replicate SAN workloads in consistency groups across sites, do not require identical storage hardware configurations at both sites. Instead, the two ONTAP clusters only need to be from the same storage families, either AFF or ASA systems, but not necessarily the same hardware model.

Note: SM-BC solutions are not supported on FAS storage systems.

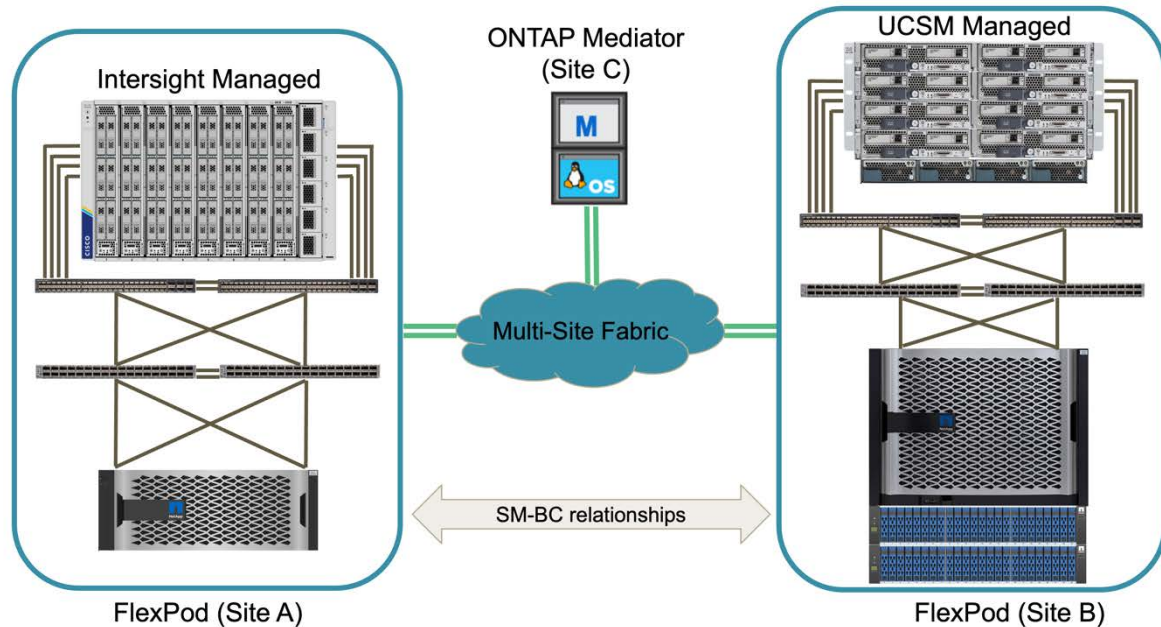
To create a FlexPod SM-BC solution, you can deploy two new FlexPod infrastructures, implement it on two existing compatible FlexPod infrastructures, or add a new FlexPod infrastructure to peer with an existing FlexPod. Figure 13 illustrates the solution components of a FlexPod SM-BC solution.

Figure 13) FlexPod SM-BC solution components.



For example, you can add a new FlexPod infrastructure to protect an existing FlexPod solution which utilizes Cisco UCS 5108 chassis and B-Series blade servers managed by Cisco UCS Manager. For the new FlexPod deployment, you can utilize the latest UCS X9508 chassis with X210c compute nodes managed by Cisco Intersight. The FlexPod at each site is connected to a larger data center fabric and the sites are connected through an interconnect network to form a multi-site fabric as shown in Figure 14.

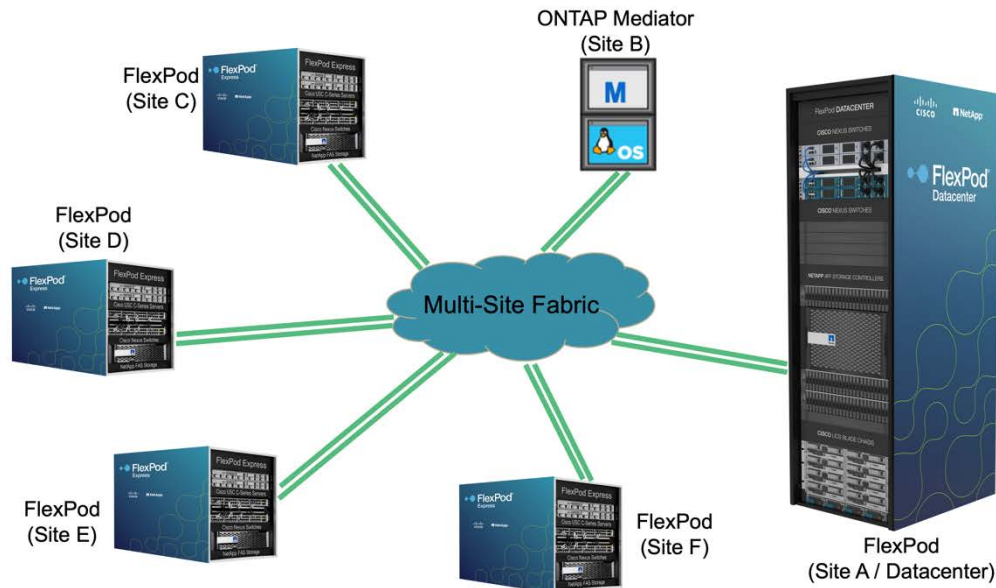
Figure 14) FlexPod SM-BC solution topology deployed with a multi-site fabric.



A good use case of the asymmetric deployment topology is to create a new solution between an existing data center and a new branch office in a metropolitan area. While the FlexPod solution in the existing data center might have significant amount of compute and storage resources, the new branch office resource requirements might be met by deploying a much smaller FlexPod.

For companies that have several branch offices in a metro area that all need to be protected to ensure business continuity, the FlexPod SM-BC deployment topology shown in Figure 15 can be implemented to protect critical application and data services to achieve zero RPO and near zero RTO objectives for the SAN workloads at all branch sites.

Figure 15) FlexPod SM-BC solution topology for a datacenter with multiple branch offices.



For this deployment model, each branch office establishes SM-BC relationships and consistency groups it requires with the datacenter in the metro area. For this type of multi-site deployment, pay careful attention to consider the supported SM-BC object limits, so the overall consistency group relationships and endpoint counts do not exceed the supported maximums at the datacenter.

FlexPod security hardening

Security has been top-of-mind for enterprises due to high-profile security incidents such as ransomware attacks which causes substantial business disruptions and financial and data losses. In addition to causing business disruptions and losses, some attackers were successful in stealing valuable private data of customers of enterprises and those incidents can cause cascading customer impacts and damage the brand image of enterprises substantially. As the frequency of attacks and the severity of the impact increase, enterprises not only need to promptly harden the security of their existing solutions but also investigate and adopt new solutions which are secure by design.

As FlexPod solutions provide the foundation infrastructure for enterprises and business across the globe, having security hardening best practices and providing insights into the tools and technologies built into the FlexPod stack to help enterprises secure their data and promptly recover from security incidents are of critical importance. This technical report was developed with securing the components of the FlexPod solutions in mind to help enterprises enhance the overall security of their business solutions.

Typical FlexPod solutions include compute, network, storage, and virtualization layers. Therefore, we examined the various aspects of the solutions and aimed to highlight and bring awareness to the available tools and technologies for securely implementing your business solutions. In some cases, we also provide concrete examples for you to adopt or provide guidance for you to consider. Some of the discussion topics span all layers of the component, while others might be specific features for achieving certain security objectives. Additional resources and information from NetApp, Cisco, and VMware should also be reviewed and adopted as appropriate to continually improve your overall security posture.

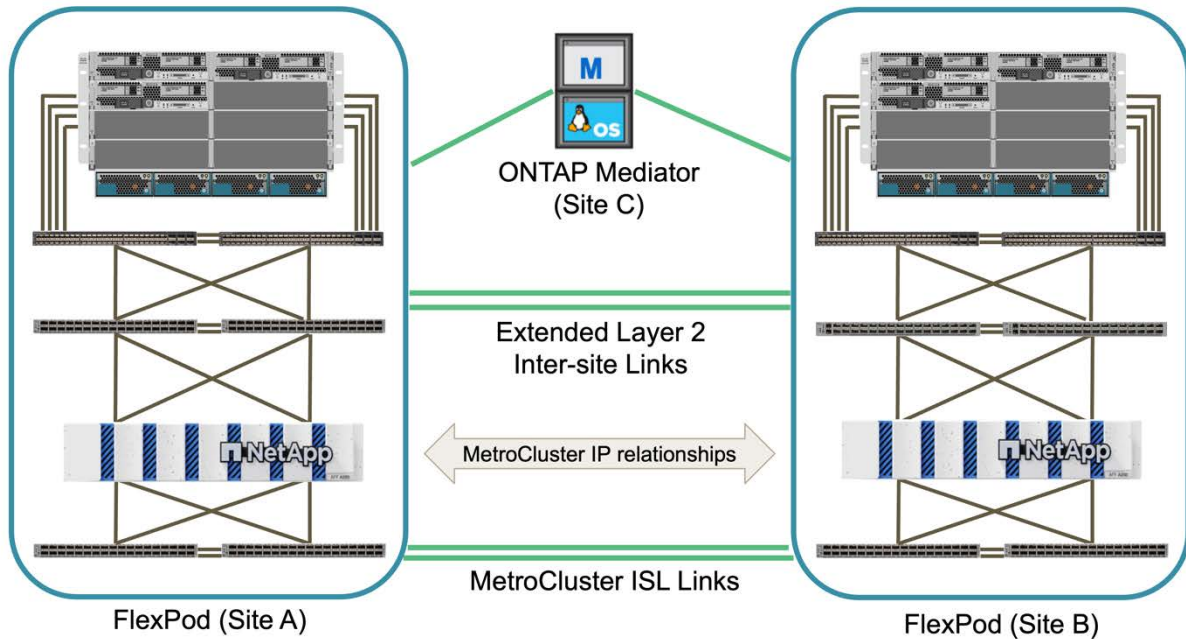
As technologies evolve and knowledge about the various attacks and vulnerabilities become public and are documented, it is also important to be up to date on those incidents and security advisories so you can better evaluate the vulnerabilities of your solutions. Keeping the software and firmware updated can help mitigate any vulnerabilities which have been addressed and adopting new security functionalities can help improve the overall security of your solution.

Validation topology

For the validation of the FlexPod solution security hardening, supported technology components from NetApp, Cisco, and VMware are utilized. The solution features NetApp AFF A250 HA pairs running ONTAP 9.13.1, dual Cisco Nexus 9336C-FX2 FlexPod switches and dual Cisco Nexus 3232C MetroCluster IP backend switches at both sites, Cisco UCS 6454 FIs at both sites, and three Cisco UCS B200 M6/M5 servers at each site running VMware vSphere 8.0 and managed by UCS Manager and VMware vCenter server.

Figure 16 shows the component level solution validation topology with two FlexPods, in a MetroCluster IP relationship, running at site A and site B connected by extended layer 2 inter-site links, MetroCluster ISL links, and an ONTAP Mediator running at site C.

Figure 16) FlexPod solution validation component-level topology.



Hardware and software

Table 2 lists the hardware and software used for the solution validation. It is important to note that Cisco, NetApp, and VMware have interoperability matrixes that should be consulted to determine support for any specific implementation of FlexPod. Click the following links for more information:

- NetApp Interoperability Matrix Tool: <http://support.netapp.com/matrix/>
- Cisco UCS Hardware and Software Interoperability Tool: <http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html>
- VMware Compatibility Guide: <http://www.vmware.com/resources/compatibility/search.php>

Table 2) Hardware and software used for solution validation.

Category	Component	Software version	Quantity
Compute	Cisco UCS Fabric Interconnect 6454	4.2(3d)	4 (2 per site)
	Cisco UCS B200 M6 servers	4.2(3d)	2 (1 per site)
	Cisco UCS B200 M5 servers	4.2(3d)	4 (2 per site)
	Cisco UCS IOM 2204XP	4.2(3d)	4 (2 per site)
	Cisco VIC 1440 (PID: UCSB-MLOM-40G-04)	5.2(3d)	2 (1 per site)
	Cisco VIC 1340 (PID: UCSB-MLOM-40G-03)	4.5(3c)	4 (2 per site)
Network	Cisco Nexus 9336C-FX2	10.2.5(M)	4 (2 per site)
	Cisco Nexus 3232C (MetroCluster IP)	9.3(11)	4 (2 per site)
Storage	NetApp AFF A250	9.13.1	4 (2 per site)
	NetApp System Manager	9.13.1	2 (1 per site)
	NetApp Active IQ Unified Manager	9.13	1
	NetApp ONTAP Tools for VMware vSphere	9.13	1
	NetApp ONTAP Mediator	1.3	1
Virtualization	VMware ESXi	8.0	6 (3 per site)
	VMware ESXi nenic Ethernet Driver	1.0.45.0	6 (3 per site)
	VMware vCenter	8.0	1
	NetApp NFS Plug-in for VMware VAAI	2.0.1	6 (3 per site)
Testing	CentOS Linux	8	1
	Microsoft Windows	10	6 (3 per site)
	IOMeter	1.1.0	6 (3 per site)

General considerations

Management plane, control plane, and data plane

When implementing a security hardening strategy for your FlexPod solution, it is important to understand what is being protected. This can typically be broken down into three areas: management plane, control plane, and data plane.

The management plane contains the traffic that supports provisioning, maintenance, and monitoring functions for the device. Example management traffic in this group includes HTTP/HTTPS, SSH, Simple Network Management Protocol (SNMP), Syslog, DNS, etc. This also includes management access to all the FlexPod components.

The control plane refers to the aspects that affect the network and communication such as switching, signaling, Link Layer Discovery Protocol (LLDP), Fiber Channel over Ethernet (FCoE), Internet Small Computer Systems Interface (iSCSI), Address Resolution Protocol (ARP), and Layer 2 keepalive.

The data plane refers to the actual information, such as the IO data between the ESXi hosts and ONTAP storage using iSCSI or NFS protocols, and the data stored on the physical storage shelves within the FlexPod system.

Protection at the management plane layer can be provided by hardening strategies such as limiting access to the devices, implementing login authentication and role-based access control that is appropriate for the solution. Protection at the control plane layer can involve utilizing appropriate security features for authentication and access and implementing access control list. On the other hand,

protection at the data plane layer can be provided by strategies such as encrypting data in transit and at rest and ensuring that the cryptographic modules in use meet the security standards and requirements.

Bastion Host

A bastion host, or a jump host, is typically a virtual machine which is hardened to provide secure access to your private FlexPod solution environment. You might implement SSH based access, or Remote Desktop Protocol (RDP) based access to the bastion host. Once you are on the bastion host, you can access your FlexPod solution environment.

Internet proxy server

Instead of giving the devices in the FlexPod solution direct internet access, which can open them up for cyber-attacks from the internet, you can place an internet proxy server between your FlexPod solution and the internet.

Disable unused services

As a security best practice, administrators should disable unnecessary services. For example, most services are disabled by default in Cisco UCS Manager Software, Cisco Nexus NX-OS software, and NetApp ONTAP software. To enable services, respective configuration commands are needed to bring the services together.

Use secure protocols

FlexPod solution management communications can contain sensitive data. As a result, secure protocols should be used whenever possible. Examples of choosing secure protocols include the use of SSH instead of Telnet and the use of HTTPS instead of HTTP so that both authentication data and management information are encrypted.

To take a step further, disable unsecure protocols after verifying that a secure alternative is available and accessible. For example, you can confirm if Telnet service is disabled on a device by trying to telnet into the device and getting refused for the connection attempt.

```
[admin@control ~]$ telnet SiteA-switch-a.nva.local
Trying 172.21.77.121...
telnet: connect to address 172.21.77.121: Connection refused
```

Network and traffic segmentation

VLANs

A VLAN is a logical segment in a switched network by function or application. Each VLAN is considered a logical network, and packets must be forwarded through a router for destinations that do not belong to the VLAN.

In FlexPod solutions, VLANs are utilized for network and traffic segmentations. Depending on the specific FlexPod solution, there are various VLANs being utilized, including out-of-band and in-band management networks, NFS, iSCSI, and NVMe/TCP protocol networks, VMware vMotion and VM traffics, and Intercluster network for ONTAP multi-cluster communications. Table 3 lists VLANs configured for the MetroCluster IP configuration utilized as the solution validation environment for this project. Figure 17 shows the VLANs configured on the UCS Manager.

Table 3) Configured VLANs and their usage.

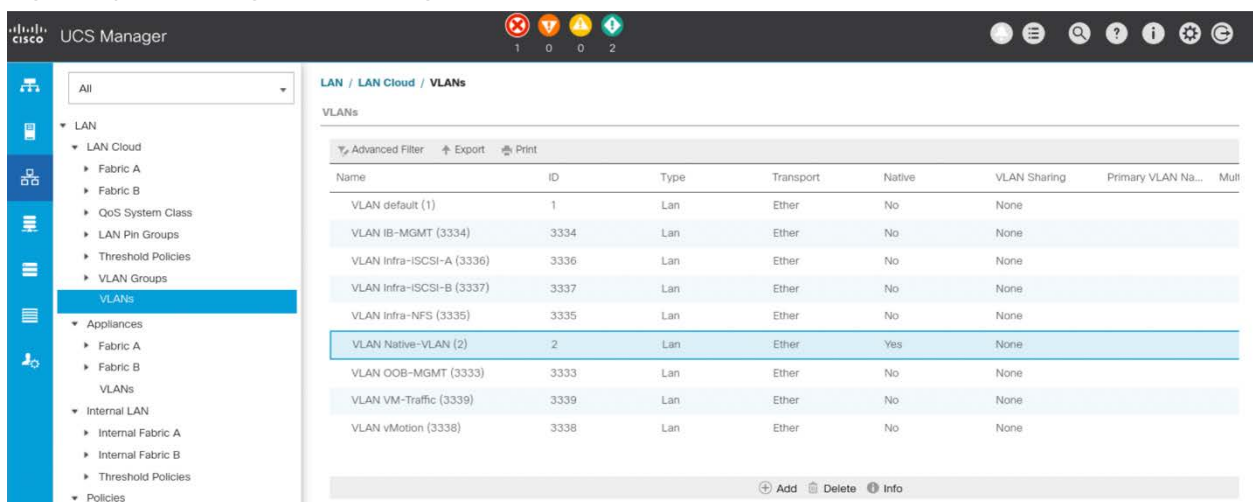
Name	VLAN ID	Usage
Native-VLAN	2	VLAN 2 used as native VLAN instead of default VLAN (1)
OOB-MGMT-VLAN	3333	Out-of-band management VLAN for devices
IB-MGMT-VLAN	3334	In-band management VLAN for ESXi hosts, VM management, etc.
NFS-VLAN	3335	NFS VLAN for NFS traffic
iSCSI-A-VLAN	3336	iSCSI-A fabric VLAN for iSCSI traffic
iSCSI-B-VLAN	3337	iSCSI-B fabric VLAN for iSCSI traffic
vMotion-VLAN	3338	VMware vMotion traffic VLAN
VM-Traffic-VLAN	3339	VMware VM traffic VLAN
Intercluster-VLAN	3340	Intercluster VLAN for ONTAP cluster peer communications

Some of the key highlights of VLAN usage are as follows:

- OOB-MGMT-VLAN allows customers to manage and access out-of-band management interfaces of various devices and is brought into the infrastructure to allow access to the Cisco UCS servers, Cisco Nexus switches, and NetApp ONTAP storage cluster. Interfaces in this VLAN are configured with MTU 1500.
- IB-MGMT-VLAN is used for in-band management of ESXi hosts, VMs, and other infrastructure services. Interfaces in this VLAN are configured with MTU 1500.
- NFS-VLAN provides ESXi hosts access to the NFS datastores hosted on the NetApp Controllers for deploying VMs. Interfaces in this VLAN are configured with MTU 9000.
- A pair of iSCSI VLANs (iSCSI-A-VLAN and iSCSI-B-VLAN) is configured to provide access to boot LUNs for ESXi hosts and iSCSI datastores. Interfaces in these VLANs are configured with MTU 9000.
- Intercluster-VLAN is configured to provide cluster peer communication between the two MetroCluster IP sites. Interfaces in these VLANs are configured with MTU 9000.

Note: If your deployment includes NVMe/TCP protocol, please refer to the FlexPod CVD design and deployment guides which utilize that protocol for additional details.

Figure 17) UCS Manager VLAN configurations.



Name	ID	Type	Transport	Native	VLAN Sharing	Primary VLAN Na...	Multi
VLAN default (1)	1	Lan	Ether	No	None		
VLAN IB-MGMT (3334)	3334	Lan	Ether	No	None		
VLAN Infra-iSCSI-A (3336)	3336	Lan	Ether	No	None		
VLAN Infra-iSCSI-B (3337)	3337	Lan	Ether	No	None		
VLAN Infra-NFS (3335)	3335	Lan	Ether	No	None		
VLAN Native-VLAN (2)	2	Lan	Ether	Yes	None		
VLAN OOB-MGMT (3333)	3333	Lan	Ether	No	None		
VLAN VM-Traffic (3339)	3339	Lan	Ether	No	None		
VLAN vMotion (3338)	3338	Lan	Ether	No	None		

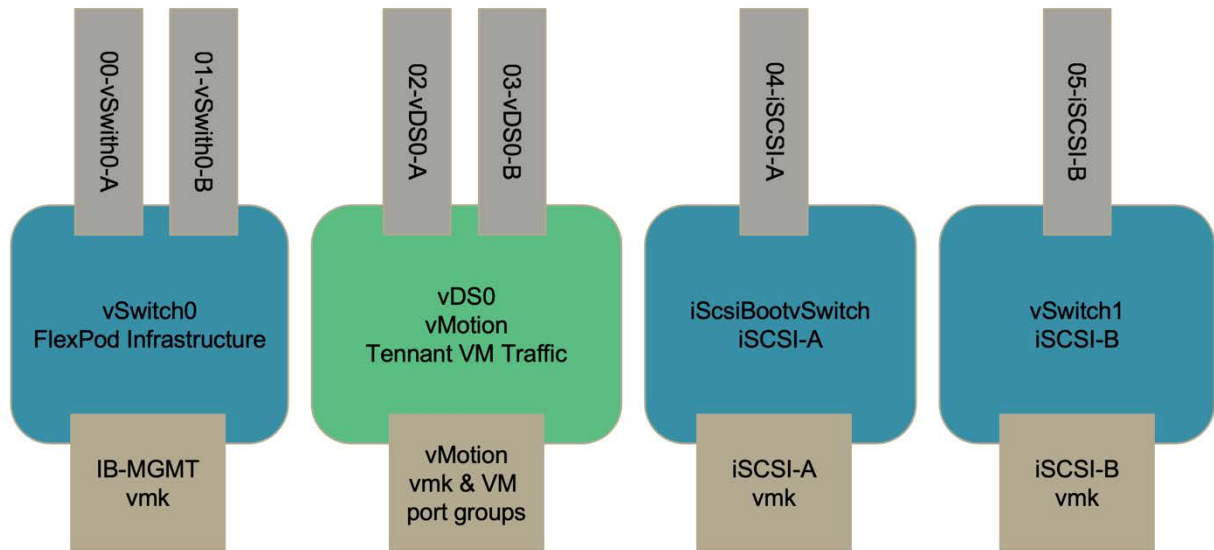
Note: The Intercluster-VLAN, VLAN 3340, is used for the ONTAP MetroCluster IP intercluster communication. As a result, it is not part of the VLANs configured on the UCS Manager.

VMware virtual networking

Each host in the cluster is deployed using identical virtual networking. The design separates the different traffic types using VMware virtual switches (vSwitch) and VMware Virtual Distributed Switches (vDS). The VMware vSwitch is used primarily for the FlexPod infrastructure networks and vDS for the application networks.

The virtual switches (vSwitch, vDS) are deployed with two uplinks per virtual switch; the uplinks at the ESXi hypervisor level are referred to as vmnics and virtual NICs (vNICs) on Cisco UCS Software. The vNICs are created on the Cisco UCS VIC adapter in each server using Cisco UCS service profiles. Six vNICs are defined, two for vSwitch0, two for vDS0, and two for the iSCSI uplinks as shown in Figure 18.

Figure 18 Virtual networking vNICs, vSwitchs, and vDS



vSwitch0 is defined during VMware ESXi host configuration, and it contains the FlexPod infrastructure management VLAN and the ESXi host VMkernel (VMK) ports for management. An infrastructure management virtual machine port group is also placed on vSwitch0 for any critical infrastructure management virtual machines that are needed.

It is important to place such management infrastructure virtual machines on vSwitch0 instead of the vDS because if the FlexPod infrastructure is shut down or power cycled and you attempt to activate that management virtual machine on a host other than the host on which it was originally running, it boots up fine on the network on vSwitch0.

The vDS contains port groups for tenant VM traffic and vMotion VMKs. The vMotion VMK is migrated to the vDS when the host is added to the vDS. Placing the vMotion VMK on the vDS allows QoS to be applied to vMotion if necessary, in the future.

Two iSCSI boot vSwitches are used in this validation. Two vNICs are configured in Cisco UCS for iSCSI boot. These vNICs use iSCSI VLAN of the appropriate fabric as the native VLAN and are attached to the appropriate iSCSI boot vSwitch.

Utilizing virtual networking with vSwitches and vDS for different type of traffic, in conjunction with appropriate VLAN configurations at the compute, network, and storage layers, to implement different network functionalities provides certain amount of network segmentation and isolation.

ONTAP IPspaces

You can use an IPspace to create a distinct IP address space for each SVM in an ONTAP storage cluster. IPspace enables clients in administratively separate network domains to access cluster data while using overlapping IP addresses from the same IP address subnet range. IP addresses defined for an IPspace are applicable only within that IPspace. A distinct routing table is maintained for each IPspace and no cross-IPspace traffic routing happens. To utilize IPspaces in ONTAP, the traffic from different clients with overlapping IP addresses will need proper networking and computer layer separations.

Network access restriction

In addition to segregating network traffic and access based on functionality. Additional limitations can be placed on a particular network segment, e.g., a particular VLAN, by only allowing access for authorized devices.

Cisco Nexus IP ACL configuration

On Cisco Nexus switches, you can configure and apply Access Control List (ACL) to filter traffic. Nexus switches support ACLs based on IPs (IPv4 and IPv6) or MAC addresses. An ACL is an ordered set of rules, where each rule specifies a set of conditions for a packet to match. The first matching rule determines whether the packet is permitted or denied. When there is no match, the applicable implicit rule is applied. The implicit rule ensures that the switch denies unmatched IP or MAC traffic.

IPv4, IPv6, and MAC ACLs also allow you to identify traffic by protocol. You can specify any protocol by number and some also by name. The created ACL filters and rules can be applied to interfaces such as ports, port channels, and VLANs.

For the validation environment, the IP addresses for the NFS VLAN falls under the 172.21.79.0/24 subnet. For simplicity, an ACL rule can be created by using the whole IP range of the NFS subnet. To have finer control, the individual NFS vmkernel IP addresses and ONTAP NFS LIFs can be called out instead.

The following examples illustrate how to create and apply an IP ACL for NFS traffic on the NFS VLAN using the whole NFS subnet IP range.

First, we create an IPv4 ACL on all the switches to allow IPs in the 172.21.79.0/24 range for both source and destination.

```
SiteA-switch-a.nva.local# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SiteA-switch-a.nva.local(config)# ip access-list acl-nfs
SiteA-switch-a.nva.local(config-acl)# permit ip 172.21.79.0/24 172.21.79.0/24
SiteA-switch-a.nva.local(config-acl)# statistics
SiteA-switch-a.nva.local(config-acl)# show ip access-lists acl-nfs

IP access list acl-nfs
    statistics per-entry
    10 permit ip 172.21.79.0/24 172.21.79.0/24
SiteA-switch-a.nva.local(config-acl)# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
SiteA-switch-a.nva.local(config-acl)# exit
SiteA-switch-a.nva.local(config)# exit
SiteA-switch-a.nva.local#
```

Next, we create a VLAN ACL (VACL) by creating an VLAN access map and associates an IP ACL with an action to be applied to the matching traffic.

```
SiteA-switch-a.nva.local# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SiteA-switch-a.nva.local(config)# vlan access-map map-nfs
```



```
SiteA-switch-a.nva.local(config-access-map)# match ip address acl-nfs
SiteA-switch-a.nva.local(config-access-map)# action forward
SiteA-switch-a.nva.local(config-access-map)# no statistics
SiteA-switch-a.nva.local(config-access-map)# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
SiteA-switch-a.nva.local(config-access-map)# exit
SiteA-switch-a.nva.local(config)# exit
SiteA-switch-a.nva.local#
```

Note: The NFS IP ACL filter needs to be consistently implemented on the FlexPod switches at both sites of the solution to ensure possible communications between NFS clients and NFS servers within each site and across sites.

Note: While the NFS IP ACL provides additional traffic filtering on top of the NFS VLAN, it does not yet completely enable NFS client and server communication. Additional NFS related configurations are needed on the NFS client and server sides to enable NFS traffic between them.

Login authentication

Password strengths and policies

Using a strong password to access and secure you FlexPod components is very important. The following is a list of guidelines for creating a strong password.

- Use a password which is at least eight characters long.
- Use a password which contains lower case letters, upper case letters, digits, and special characters.
- Use a password which does not contain many consecutive characters or numbers.
- Use a password which does not contain many repeating characters or numbers.
- Use a password which does not contain dictionary words or proper names.
- Use a password which is not identical to the username or the reverse of the username.
- Check documentation for the specific password characters which are not allowed by the specific FlexPod components.

In addition to using a strong password, it is a best practice to change passwords regularly and to use password policies to enforce the required password changes. Please consult documentation for details on implementing password policies.

Lightweight Directory Access Protocol authentication

The Lightweight Directory Access Protocol (LDAP) provides centralized validation of users attempting to gain access to a device. For a FlexPod environment with a lot of users, using LDAP is recommended to simplify and centralize login authentication. In addition to authentication, LDAP also supports authorization for role-based access control.

Cisco UCS Manager login authentication

Cisco UCS Manager supports both local and remote user authentication. When using local user authentication, the user accounts exist locally in the UCS Manager. For remote user authentication, UCS Manager supports Lightweight Directory Access Protocol (LDAP), Remote Access Dial-In User Service (RADIUS), and Terminal Access Controller Access Control System Plus (TACACS+) protocols.

To support remote authentication, you must create a provider for the remote service so UCS Manager can communicate with the system providing the authentication. For RADIUS and TACACS+ authentications, you must configure user roles and locales. For LDAP, LDAP Group Mapping can be used to assign roles and locales.

Two-factor authentication is supported for RADIUS or TACACS+ by associating provider groups with designated authentication domains and enabling two-factor authentication for those domains. Two-factor authentication is not supported when using local or LDAP authentications.

Local authentication

During the initial setup for the default admin user account, a password is chosen. For additional users to access the system, create a unique username and password for each one. You can configure up to 48 local user accounts in each Cisco UCS Manager domain.

RADIUS authentication

Before configuring the RADIUS features on your UCS Manager, you should already have a RADIUS server and have configured users with the attribute that holds the user role and locale information for UCS Manager.

You can create a RADIUS provider on UCS Manager under User Management. You can configure a RADIUS provider group if the implementation involves multiple RADIUS databases. UCS Manager supports up to 16 RADIUS providers.

TACACS+ authentication

UCS Manager supports up to 16 TACACS+ providers. Before configuring the TACACS+ features on your UCS Manager, you should already have a TACACS+ server configured. On the TACACS+ server, you will need to create the cisco-av-pair attribute, which is the string that provides the attribute ID to the TACACS+ provider of UCS Manager.

LDAP authentication

UCS Manager supports up to 16 LDAP providers. Before configuring the LDAP features on your UCS Manager, you should already have an LDAP server configured and have users and LDAP groups created with user role and locale information. For secure communication between the UCS Manager and the LDAP server, create a trusted point containing the certificate of the LDAP server in UCS Manager.

Cisco Nexus login authentication

Cisco NX-OS devices support local authentication and remote authentication using one or more RADIUS or TACACS+ servers. It is part of the Authentication, Authorization, and Accounting (AAA) feature for user identity verification, access permission, and activity reporting. The password-strength checking is enabled by default on NX-OS to prevent weak passwords. It uses SHA256 as the hashing algorithm for password encryption.

Local authentication

On the Cisco NX-OS devices, you can create and manage users accounts and assign roles that limit access to operations. Up to a maximum of 256 user accounts can be created. In addition, you can configure the expire option which determines the date when the user account is disabled.

RADIUS authentication

RADIUS client which runs on the NX-OS devices can send authentication requests to a RADIUS server that contains user authentication information. When the transmission to a RADIUS server timed out, the authentication is reverted to the local authentication.

On the Cisco NX-OS devices, you can also enable RADIUS server feature for it to act as a central RADIUS server for RADIUS client login authentication.

TACACS+ authentication

TACACS+ security protocol can provide centralized authentication for users to access a NX-OS device. The TACACS+ client/server protocol uses TCP port 49. In addition, TACACS+ provides separate facilities for authorization, and accounting. While the RADIUS protocol only encrypts passwords, the TACACS+ encrypts the entire protocol payload between the switch and the AAA server. You must configure a TACACS+ server before configuring the TACACS+ features on your NX-OS device.

LDAP authentication

LDAP provides centralized validation of users attempting to gain access to a device. LDAP can provide support for both authentication and authorization. The LDAP client/server protocol uses TCP port 389. You must have configured an LDAP server before configuring the LDAP features on your Nexus device.

Password encryption

NX-OS supports strong, reversible 128-bit Advanced Encryption Standard (AES) password encryption, also known as type-6 encryption. AES password encryption is not enabled by default. The following example shows how to configure a master encryption key, which is used to encrypt and decrypt passwords, and enable the AES password encryption.

```
SiteA-switch-a.nva.local# key config-key ascii
New Master Key:
Retype Master Key:

SiteA-switch-a.nva.local# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SiteA-switch-a.nva.local(config)# feature password encryption aes
SiteA-switch-a.nva.local(config)# show encryption service stat
Encryption service enabled
Master Encryption Key configured
Type-6 encryption is being used
SiteA-switch-a.nva.local(config)# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
SiteA-switch-a.nva.local(config)# exit
SiteA-switch-a.nva.local#
```

Note: The Master-key length should be in between 16 to 64 chars(inclusive).

Note: AES password encryption is supported for the RADIUS and TACACS+ applications.

Certificate-based authentication

Cisco NX-OS supports certificate-based authentication for ssh access. The following highlights the configuration steps needed to enable certificate-based authentication for the default admin user.

Use OpenSSL on a Linux machine to generate a certificate.

```
[admin@control ~]$ openssl req -x509 -nodes -days 2190 -newkey rsa:2048 -keyout admin.key -out
admin.pem -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=admin"
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'admin.key'
-----
```

Note: The above command generates a public certificate named admin.pem and a private key named admin.key. The common name (CN) corresponds to the NX-OS user ID admin.

Log in to the switch and use the SCP protocol to copy the public certificate into the switch's bootflash.

```
SiteA-switch-a.nva.local# copy scp://admin@10.61.177.2//home/admin/admin.pem bootflash:admin.pem
Enter vrf (If no input, current vrf 'default' is considered): management
Inbound-ReKey for 10.61.177.2:22
```

```
admin@10.61.177.2's password:
admin.pem                               100% 1257      1.1MB/s   00:00
Copy complete, now saving to disk (please wait)...
Copy complete.
```

Enter global configuration mode, configure the public certificate file in bootflash as the sshkey, check the user account configuration, and save the configuration changes.

```
SiteA-switch-a.nva.local# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SiteA-switch-a.nva.local(config)# username admin sshkey file bootflash:admin.pem

SiteA-switch-a.nva.local(config)# show user-account admin
user:admin
    this user account has no expiry date
    roles:network-admin
    ssh public key: ssh-rsa
AAAAB3NzaClyc2EAAAADAQABAAQDAMIz0O26v/eM3ksVi63v+Q/FvqlIYZbforxCNf
sQDj5aogTlsylm9a8QF+S2o/ykii5BkLJ6NzUODoFXUjAGY3hNlxgIisatcqWxxMq3zwGoWHQ53Lq4Ct2SZQ4aHgyYdEkoOO
ck0G7
4X0REMqB4kqyoILU5PKb0zmicapCsC8Er87E0gK/xrStrWwUKJJ5jmjSe4ZL99+qYf6U+gpkZi2sZXK6ai/dEOqKpapYbVv/
E/ZqP
6iLBsn0exLXYduRhKDAENYhEdMUEkIYfgVOV8KS/AxPg2OSH9E1KLS8WRUSMe/IoEbSAbcDp2nyUZxUOPZWk79Cd9zgCv3Fc9
B

SiteA-switch-a.nva.local(config)# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
SiteA-switch-a.nva.local(config)# exit
```

Now that the certificate-based authentication is configured on the switch for the admin user. The admin user can use ssh to interact with the switch by using certificate-based authentication and without specifying a password. See below for an example of gathering the system uptime information from the switch by using this authentication approach.

```
[admin@control ~]$ ssh -i admin.key admin@SiteA-switch-a.nva.local "show system uptime"
Access restricted to authorized users ONLY!
System start time:      Sun Aug 27 03:32:19 2023
System uptime:         52 days, 16 hours, 25 minutes, 4 seconds
Kernel uptime:         52 days, 16 hours, 27 minutes, 18 seconds
```

Instead of specifying the private key with the `-i` identify file flag, you can also copy the content of the user's private key file and save it as the user's ssh identify file `.ssh/id_rsa`. Afterwards, the ssh command can locate the identify file information automatically from the default location without needing to specify it as a command line parameter.

```
[admin@control ~]$ cp admin.key ~/.ssh/id_rsa

[admin@control ~]$ ssh admin@SiteA-switch-a.nva.local "show system uptime"
Access restricted to authorized users ONLY!
System start time:      Sun Aug 27 03:32:19 2023
System uptime:         52 days, 16 hours, 28 minutes, 20 seconds
Kernel uptime:         52 days, 16 hours, 30 minutes, 35 seconds
```

NetApp ONTAP login authentication

For ONTAP storage, you can enable local or remote cluster and Storage Virtual Machine (SVM) administrator accounts. A local account is one in which the account information, public key, or security certificate resides on the storage system. For remote accounts, the account information is stored remotely. For example, AD account information is stored on a domain controller and LDAP and NIS accounts reside on LDAP and NIS servers.

A cluster administrator accesses the admin SVM for the cluster. The admin SVM and a cluster administrator with the reserved name admin are automatically created when the cluster is set up. A

cluster administrator with the default admin role can administer the entire cluster and its resources. The cluster administrator can create additional cluster administrators with different roles as needed. An SVM administrator accesses a data SVM. The cluster administrator creates data SVMs and SVM administrators as needed.

Local authentication

You can configure ONTAP to create administrator accounts to access the admin SVM or data SVMs with a password. You are prompted for the password after you enter the account creation command. During account creation, you can optionally assign an access control role to the account. If you are unsure of the access control role that you want to assign to a login account, you can use the `security login modify` command to add/update the role for the account later.

Beginning with ONTAP 9.13.1, you can associate an X.509 certificate with the public key that you associate with the administrator account. This gives you the added security of certificate expiration or revocation checks upon SSH login for that account.

Active directory authentication

You can configure ONTAP to enable Active Directory (AD) user or group accounts to access the admin SVM or data SVMs. Any user in the AD group can access the SVM with the role that is assigned to the group.

You must configure AD domain controller access to the cluster or SVM before an AD account can access the SVM. To use AD domain controller for authentication, the ONTAP cluster time must be synchronized to within five minutes of the time on the AD domain controller.

You can use an SSH public key as either your primary or secondary authentication method with an AD user password. However, if you choose to use an SSH public key as your primary authentication, no AD authentication takes place.

LDAP or NIS authentication

You can configure ONTAP to enable LDAP or NIS user accounts to access the admin SVM or data SVMs. You must configure LDAP or NIS server access to the SVM before the account can access the SVM. Multifactor authentication is also supported for remote users using LDAP or NIS servers for authentication.

SAML authentication

You can configure Security Assertion Markup Language (SAML) authentication for web services. When SAML authentication is configured and enabled, users are authenticated by an external Identity Provider (IdP) instead of the directory service providers such as Active Directory and LDAP.

SAML authentication applies only to the `http` and `ontapi` applications, which are used by the Service Processor Infrastructure, ONTAP APIs, or System Manager web services. In addition, SAML authentication is applicable only for accessing the admin SVM.

Application methods

The `security login create` command creates a login method for the management utility. A login method consists of a username, an application (access method), and an authentication method. It can optionally include an access-control role name.

The application method specifies the access type of the login method. Possible values include `amqp`, `console`, `http`, `ontapi`, `rsh`, `snmp`, `service-processor`, `ssh`, and `telnet`. A username can be associated with multiple applications. However, application access should be limited only to what the user requires.

Setting this parameter to service-processor grants the user access to the Service Processor. When this parameter is set to service-processor, the `-authentication-method` parameter must be set to password because the Service Processor only supports password authentication. SVM user accounts cannot access the Service Processor. Therefore, operators and administrators cannot use the `-vserver` parameter when this parameter is set to service-processor.

For security reasons, Telnet and Remote Shell (RSH) are disabled by default because NetApp recommends Secure Shell (SSH) for secure remote access. If there is a requirement or unique need for Telnet or RSH, they can be enabled.

Multi-factor authentication

Multifactor authentication (MFA) allows you to enhance security by requiring users to provide two authentication methods to log in to an admin or data SVM. Depending upon your version of ONTAP, you can use a combination of an SSH public key, user password, and time-based one-time password (TOTP) to set up multifactor authentication.

As an example, let's create a new administrator `fpadmin` who is allowed to ssh into the cluster and configure a combination of password and public key for two-factor authentication.

Use the `ssh-keygen` command in Linux to create a public/private key pair for the `fpadmin` user. The key type used here is `ecdsa-sha2-nistp256` which is supported even when the more secure Federal Information Processing Standard (FIPS) 140 compliant mode is enabled for the cluster. Enter a passphrase when prompted.

Note: Please see the FIPS 140 compliance section for information on FIPS mode.

```
[fpadmin@control ~]$ ssh-keygen -t ecdsa-sha2-nistp256
Generating public/private ecdsa-sha2-nistp256 key pair.
Enter file in which to save the key (/home/fpadmin/.ssh/id_ecdsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/fpadmin/.ssh/id_ecdsa.
Your public key has been saved in /home/fpadmin/.ssh/id_ecdsa.pub.
The key fingerprint is:
SHA256:BzjLTvfRLONbhBdfA9C2G9JRTlie6nWH6ee/WIKQMzI fpadmin@control.nva.local
The key's randomart image is:
+---[ECDSA 256]---+
|      .o..+o|
|      .   +ooo|
|     o .  + oo+|
|    . o ..= *.+.|
|   +ES=* *.*.o|
|  o .o++*oo. o|
|   .  o..o...|
|      o  +o|
|      .  .|=|
+-----[SHA256]-----+

[fpadmin@control ~]$ cat /home/fpadmin/.ssh/id_ecdsa.pub
ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJ82GgWpaT4pz9YeT0azbo49lHda+de55xVKhuJoTx4Vc
rLAZeZs/Ghf2aXOXEsTc3Zy8WD6T5aIMW0sQCc+Qdc= fpadmin@control.nva.local
```

Create the new `fpadmin` user in ONTAP using the `security login create` command, specify `ssh` as the application and use both password and publickey authentication methods. You can use the `security login show` command to check on the user login configuration.

```
SiteA::> security login create -user-or-group-name fpadmin -application ssh -authentication-
method password -second-authentication-method publickey
Please enter a password for user 'fpadmin':
Please enter it again:
Warning: To use public-key authentication, you must create a public key for user "fpadmin".
SiteA::> security login show -user-or-group-name fpadmin
```

Vserver: SiteA

User/Group		Authentication		Acct	Second
Name	Application	Method	Role Name	Locked	Authentication Method
fpadmin	ssh	password	admin	no	publickey

To create the public key in ONTAP for the fpadmin user, use the `security login publickey create` command and provide the associated parameters, including the public key from the `id_ecdsa.pub` file generated above.

```
SiteA::> security login publickey create -username fpadmin -index 0 -publickey "ecdsa-sha2-
nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJ82GgWpaT4pz9YeT0azbo49lHda+de55xVKhuJoTx4Vc
rLazZeZs/Ghf2aXOXEsTc3Zy8WD6T5aIMW0sQCc+Qdc= fpadmin@control.nva.local" -vserver SiteA
```

After the two-factor authentication is configured, the fpadmin user can login to the ONTAP cluster with the needed SSH key in place and the correct password as shown below.

```
[fpadmin@control ~]$ ssh fpadmin@SiteA.nva.local
The authenticity of host 'sitea.nva.local (172.21.77.100)' can't be established.
ECDSA key fingerprint is SHA256:+uSpzpQl+9GiDbjs4l7dTYgVMbTL0wTY9pGUKM4HP2g.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'sitea.nva.local,172.21.77.100' (ECDSA) to the list of known hosts.
Access restricted to authorized users ONLY!
Password:

Last login time: 10/10/2023 23:11:19
SiteA::>
```

To test whether the public key authentication was being used as part of the login process above, we can move the keys out of the default directory into a temporary directory and then attempt to login again.

```
[fpadmin@control ~]$ cd .ssh
[fpadmin@control .ssh]$ ls
id_ecdsa id_ecdsa.pub known_hosts
[fpadmin@control .ssh]$ mkdir tmp
[fpadmin@control .ssh]$ cd tmp
[fpadmin@control tmp]$ mv ../id* .
[fpadmin@control tmp]$ cd ..
[fpadmin@control .ssh]$ ls
known_hosts tmp
[fpadmin@control .ssh]$ cd

[fpadmin@control ~]$ ssh fpadmin@SiteA.nva.local
Access restricted to authorized users ONLY!
fpadmin@sitea.nva.local: Permission denied (publickey).
[fpadmin@control ~]$
```

As the example above shows, when the SSH key information is not provided, the ssh login attempt was rejected with a reason of `Permission denied (publickey)` and the user is no longer prompted for a password.

With ONTAP 9.13.1, you can configure password or SSH public key as the first authentication method and use time-based one-time password (TOTP) as the secondary password. You must configure your TOTP app to work with your smartphone and create your TOTP secret key. TOTP is supported by various authenticator apps such as Google Authenticator. With ONTAP 9.12.1 and later, you can use Yubikey hardware authentication devices for SSH client MFA using the FIDO2 (Fast IDentity Online) or Personal Identity Verification (PIV) authentication standards.

Insecure ciphers

The SSH key exchange algorithms, or ciphers, with the suffix CBC are considered insecure. As a best practice, invoke the ONTAP command `security ssh remove` to remove the CBC ciphers as shown in the following example.

```
SiteA::> security ssh remove -vserver SiteA -ciphers aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc
```

Note: If the users do not perform the above task, they will see a warning in Active IQ® Unified Manager saying “SSH is using insecure ciphers.”

Enhanced SHA-512 password hash

Secure Hash Algorithm 2 (SHA-2) is a set of cryptographic hash functions. SHA-2 was first published by the National Institute of Standards and Technology (NIST) as a U.S. federal standard. The algorithms of the SHA-2 family are named after their digest lengths in bits, e.g., SHA-256 and SHA-512.

ONTAP 9 supports the SHA-2 password hash function and defaults to using SHA-512 for hashing newly created or changed passwords. We can check whether the newly created `fpadmin` account is using the SHA-512 hash with the `security login show` command in advanced privilege mode as shown in the example below.

```
SiteA::> set advanced

Warning: These advanced commands are potentially dangerous; use them only when directed to do so
by NetApp personnel.
Do you want to continue? {y|n}: y

SiteA::*> security login show -user-or-group-name fpadmin -fields hash-function
vserver user-or-group-name application authentication-method remote-switch-ipaddress hash-
function
-----
-
SiteA  fpadmin          ssh          password          -          sha512

SiteA::*> set admin

SiteA::>
```

Note: Administrator accounts created prior to ONTAP 9.0 continue to use MD5 password hash after the upgrade until the passwords are manually changed. By running the `security login show -fields hash-function` command in advanced mode, you can check for user passwords which are not using the sha512 has-function. If there are, you can expire the passwords for those user accounts to force a password change during their next login. Please see ONTAP documentation for additional details.

Certificate-based authentication

When using the NetApp Manageability SDK API access to ONTAP, you must use certificate-based authentication instead of the user ID and password authentication. The following highlights the step of generating and using certificate-based access for ONTAP REST API.

Use OpenSSL to generate a certificate by running the following command.

```
[fpadmin@control ~]$ openssl req -x509 -nodes -days 2190 -newkey rsa:2048 -keyout fpadmin.key -
out fpadmin.pem -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=fpadmin"
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'fpadmin.key'
-----
```

Note: The above command generates a public certificate named `fpadmin.pem` and a private key named `fpadmin.key`. The common name (CN) corresponds to the ONTAP user ID `fpadmin`.

Install the contents of the public certificate in privacy enhanced mail (pem) format in ONTAP by running the following command and pasting the certificate's contents when prompted.

```
SiteA::> security certificate install -type client-ca -vserver SiteA

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIDdzCCA1+gAwIBAgIUYtcDyqbFYR0U26x8PBDGcEvZHScwDQYJKoZIhvcNAQEL
BQAwSzELMAkGA1UEBhMCVVMxChZAJBgNVBAGMAk5DMQwwCgYDVQQHDANSVFAXDzAN
BgNVBAoMBk5ldEFwcDEQMA4GA1UEAwMHZnBhZG1pbjBjAeFw0yMzEwMTcxODEwMDFa
...
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for future reference.

The installed certificate's CA and serial number for reference:
CA: fpadmin
serial: 62D703CAA6DF611D14DBAC7C3C10C6704BD91D27

The certificate's generated name for reference: fpadmin
```

Note: The entire certificate, including the BEGIN CERTIFICATE and END CERTIFICATE lines, from the public certificate file should be pasted when prompted. Some lines from the certificate file have been omitted in the example above.

Configure ONTAP to allow client access through SSL and add the http application for the ONTAP REST API access for the fpadmin user as shown in the example below.

```
SiteA::> security ssl modify -vserver SiteA -client-enabled true

SiteA::> security login create -user-or-group-name fpadmin -application http -authentication-
method cert -role admin -vserver SiteA
```

Issue the following command on the Linux client to query the ONTAP version to confirm using certificate for REST API access to ONTAP.

```
[fpadmin@control ~]$ curl -k --cert-type PEM --cert ./fpadmin.pem --key-type PEM --key ./fpadmin.key -X GET "https://SiteA.nva.local/api/cluster?fields=version"
{
  "version": {
    "full": "NetApp Release 9.13.1P1: Tue Jul 25 10:19:28 UTC 2023",
    "generation": 9,
    "major": 13,
    "minor": 1
  },
  "_links": {
    "self": {
      "href": "/api/cluster"
    }
  }
}
```

VMware vSphere login account and authentication

ESXi local authentication

After initial ESXi installation, only the root user can log in to the Direct Console User Interface (DCUI) and the ESXi Shell and the SSH services are disabled by default. You can enable ESXi Shell for troubleshooting and enable SSH for remote access to the ESXi host. You should activate the ESXi Shell for troubleshooting only to reduce the risk of unauthorized access.

vCenter server single sign-on authentication

vCenter server includes an identity provider and uses vsphere.local domain as the identify source for local account by default. The domain information can be customized during vCenter server installation.

Authentication of users is through either external identity provider federation or the vCenter Server built-in identity provider. The built-in identity provider supports local accounts,

You can enable federated authentication and configure an external identity provider to replace vCenter Server as the identity provider. vCenter Server 7.0 and later supports Active Directory or OpenLDAP. The support for Okta identity management service starts in vSphere 8 update 1.

Role-based access control

With role-based access control (RBAC), users can be configured to have access to only the systems and privileges required for their job roles and functions. The FlexPod component software include predefined user roles and privileges that can be used for the various needs. Customizations are also available to define custom roles using various privileges to meet the specific needs.

Cisco UCS Manager role-based access control

In Cisco UCS Manager, you do not directly assign privileges to users. Instead, you assign the roles, which contain one or more privileges, to the users. In order to properly assign a role to a user, you need to know which system resources the privileges included in that role allow the user to access.

You can divide the large physical infrastructure of a Cisco UCS domain into logical entities called organizations to achieve a logical isolation between organizations without providing a dedicated physical infrastructure for each organization. You can assign unique resources to each tenant through the related organization in the multi-tenant environment.

These resources can include different policies, pools, and quality of service definitions. You can also implement locales to assign or restrict user privileges and roles by organization, if you do not want all users to have access to all organizations. A Cisco UCS domain can contain up to 48 user roles and 48 user locales. Table 4 and Table 5 below shows example predefined user roles and privileges for the Cisco UCS Manager software.

Table 4) Example predefined user roles for Cisco UCS Manager software.

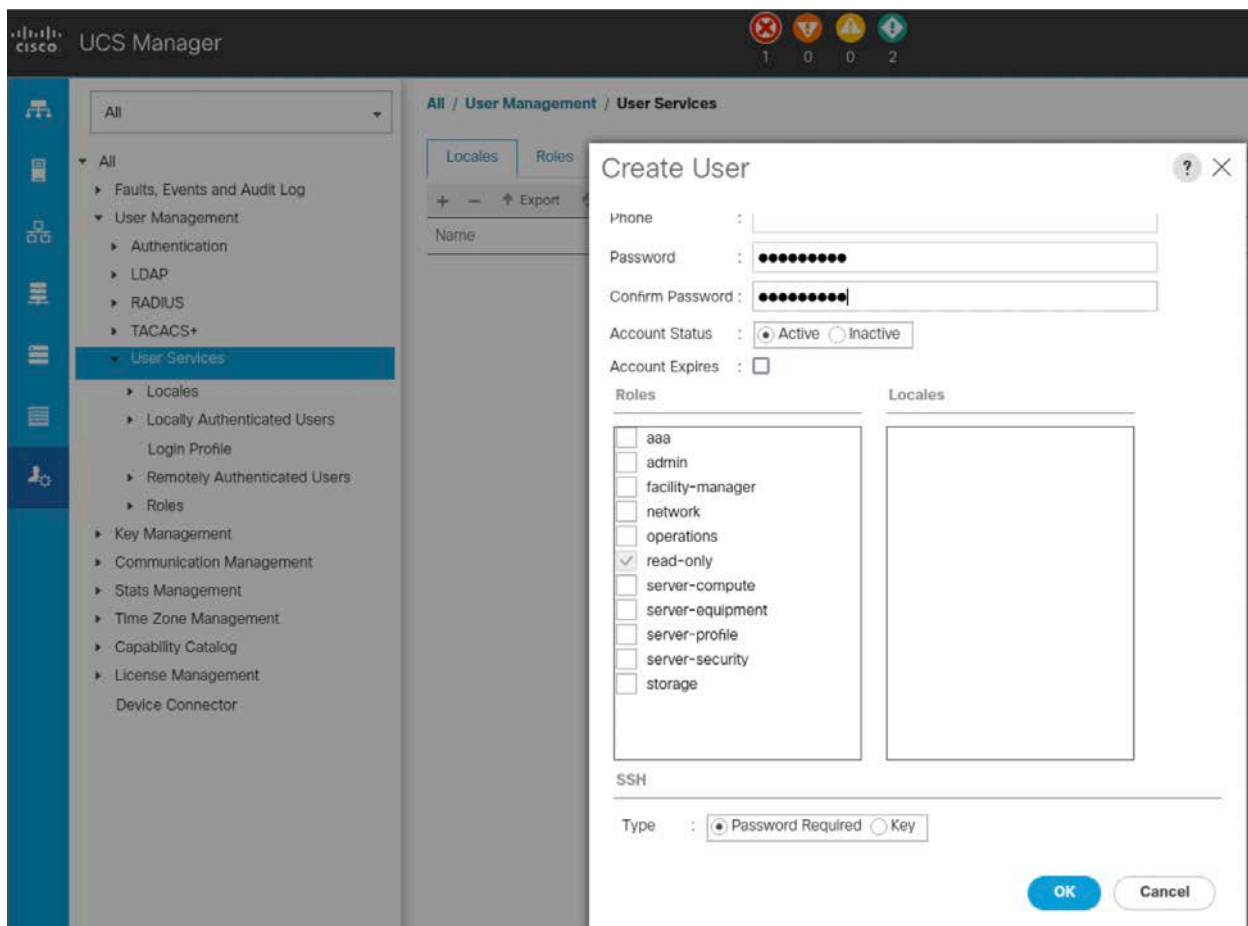
User role	Capabilities
Administrator	<ul style="list-style-type: none">Complete read-and-write access to the entire system. You cannot change it.
Server Equipment Administrator	<ul style="list-style-type: none">Read-and-write access to physical server-related operations. Read access to the remaining system.
Server Profile Administrator	<ul style="list-style-type: none">Read-and-write access to logical server-related operations. Read access to the remaining system.
Server Security Administrator	<ul style="list-style-type: none">Read-and-write access to server security-related operations. Read access to the remaining system.
Network Administrator	<ul style="list-style-type: none">Read-and-write access to fabric interconnect infrastructure and network security operations. Read access to the remaining system.
Storage Administrator	<ul style="list-style-type: none">Read-and-write access to storage operations. Read access to the remaining system.
Operations	<ul style="list-style-type: none">Read-and-write access to systems logs, including the syslog servers, and faults. Read access to the remaining system.
Read-Only	<ul style="list-style-type: none">Read-only access to system configuration with no privileges to modify the system state.

Table 5) Example user privileges for Cisco UCS Manager software.

Privilege	Description	Default role assignment
admin	System administration	Administrator
server-equipment	Server hardware equipment	Server Equipment Administrator
server-maintenance	Server maintenance	Server Equipment Administrator
server-policy	Server policy	Server Equipment Administrator
service-profile-config	Service profile configuration	Server Profile Administrator
service-profile-config-policy	Service profile configuration policy	Server Profile Administrator
service-profile-ext-access	Service profile endpoint access	Server Profile Administrator
server-security	Server security	Server Security Administrator
service-profile-security	Service profile security	Server Security Administrator
service-profile-security-policy	Service profile security policy	Server Security Administrator
service-profile-network	Service profile network	Network Administrator
service-profile-network-policy	Service profile network policy	Network Administrator
service-profile-qos	Service profile qos	Network Administrator
service-profile-qos-policy	Service profile qos policy	Network Administrator
service-profile-storage	Service profile storage	Storage Administrator
service-profile-storage-policy	Service profile storage policy	Storage Administrator
read-only	Read-only access. Read-only cannot be selected as a privilege; it is assigned to every user role.	Read-Only

Cisco recommends that you create users for server administrator account, network administrator account, and storage administrator account. The following provides the steps for creating a user account and assigns the role of read-only to the account.

Log in to UCS Manager GUI, click Admin in the Navigation pane, expand All > User Management > User Services, right-click User Services and choose Create User to open the User Properties dialog box. Complete the following fields as appropriate: Login ID, First and Last names, Email, Phone, Password, Confirm Password, and Account Status. Select one or more boxes to assign roles in the Roles area, select Password Required or Key to enter password or ssh Key for SSH Type, click OK to complete, and click OK again on the success pop-up message.



Cisco Nexus role-based access control

In Cisco Nexus, rule is the basic element of a role. The rules contained in a user role define the allowed operations for the user who is assigned the role. Each user can have multiple roles and each user role can contain multiple rules. Table 6 lists the Cisco NX-OS software user roles.

Table 6) Example predefined user roles for Cisco NX-OS software.

User role	Capabilities
network-admin	<ul style="list-style-type: none"> Predefined network admin role has access to all commands on the switch.
network-operator	<ul style="list-style-type: none"> Predefined network operator role has access to all read commands on the switch.
vdc-admin	<ul style="list-style-type: none"> Predefined vdc admin role has access to all commands within a VDC instance.
vdc-operator	<ul style="list-style-type: none"> Predefined vdc operator role has access to all read commands within a VDC instance.
dev-ops	<ul style="list-style-type: none"> Predefined system role for devops access. This role cannot be modified.

Note: The Cisco Nexus 9000 Series switches support a single virtual device context (VDC). As a result, the vdc-admin has the same privileges and limitations as the network-admin and the vdc-operator has the same privileges and limitations as the network-operator.

You can apply rules for commands, features, feature groups, and object identifiers. Access restrictions can be assigned for specific virtual routing and forwarding instances (VRFs), VLANs, and interfaces. See below for a few limitations of using RBAC and refer to the Cisco Nexus NX-OS documentation for complete guidelines and restriction details.

- A user account can have up to 64 user roles.
- A user role can have up to 256 rules.
- You cannot remove the default user roles from the default admin user accounts.

See below for an example of creating a read-only user with network-operator role which has complete read access to the device.

```
SiteA-switch-a.nva.local# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SiteA-switch-a.nva.local(config)# username fpmonitor password Als2D4f5! role network-operator
SiteA-switch-a.nva.local(config)# exit
SiteA-switch-a.nva.local# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
```

For the next example, we create another admin user with username fpadmin, who is assigned the network-admin role and has complete control of the device.

```
SiteA-switch-a.nva.local# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SiteA-switch-a.nva.local(config)# username fpadmin password Als2D4f5! role network-admin
SiteA-switch-a.nva.local(config)# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
SiteA-switch-a.nva.local(config)# exit
SiteA-switch-a.nva.local#
```

NetApp ONTAP role-based access control

The RBAC solution in ONTAP limits users' administrative access to the level granted for their defined role, which allows administrators to manage users by assigned role. ONTAP provides several predefined roles, and you can also create custom roles as necessary.

By default, a cluster administrator is assigned the predefined admin role. For the administration of the created Storage Virtual Machine (SVM), the default vsadmin account can be enabled for SVM specific management. There are also predefined SVM administrator roles that can be utilized. Table 7 and Table 8 list the example predefined roles for ONTAP cluster administrators and ONTAP SVM administrators.

Table 7) Example predefined roles for ONTAP cluster administrators.

Cluster role	Level of access	Capabilities
admin	all	All command directories (DEFAULT)
autosupport	all	<ul style="list-style-type: none"> • set system node • autosupport
	none	All other command directories (DEFAULT)
backup	all	vserver services ndmp
	readonly	volume
	none	All other command directories (DEFAULT)
readonly	all	Evokes all show commands and resets its own password

Cluster role	Level of access	Capabilities
	readonly	<ul style="list-style-type: none"> security login password For managing own user account local password and key information only <ul style="list-style-type: none"> set
	none	All other command directories (DEFAULT)
none	none	All command directories (DEFAULT)

Note: The autosupport role is assigned to the predefined autosupport account, which is used by AutoSupport® OnDemand. ONTAP prevents you from modifying or deleting the autosupport account. ONTAP also prevents you from assigning the autosupport role to other user accounts.

Table 8) Predefined roles for ONTAP SVM administrators.

Cluster role	Capabilities
vsadmin	<ul style="list-style-type: none"> Managing own user account local password and key information Managing volumes, except volume moves Managing quotas, qtrees, Snapshot® copies, and files Managing LUNs Performing SnapLock operations, except privileged delete Configuring protocols: NFS, SMB, iSCSI, and FC, including FCoE Configuring services: DNS, LDAP, and NIS Monitoring jobs Monitoring network connections and network interface Monitoring the health of the SVM
vsadmin-volume	<ul style="list-style-type: none"> Managing own user account local password and key information Managing volumes, except volume moves Managing quotas, qtrees, Snapshot copies, and files Managing LUNs Configuring protocols: NFS, SMB, iSCSI, and FC, including FCoE Configuring services: DNS, LDAP, and NIS Monitoring network interface Monitoring the health of the SVM
vsadmin-protocol	<ul style="list-style-type: none"> Managing own user account local password and key information Configuring protocols: NFS, SMB, iSCSI, and FC, including FCoE Configuring services: DNS, LDAP, and NIS Managing LUNs Monitoring network interface Monitoring the health of the SVM
vsadmin-backup	<ul style="list-style-type: none"> Managing own user account local password and key information Managing NDMP operations Making a restored volume read/write Managing SnapMirror relationships and Snapshot copies Viewing volumes and network information
vsadmin-snaplock	<ul style="list-style-type: none"> Managing own user account local password and key information Managing volumes, except volume moves Managing quotas, qtrees, Snapshot copies, and files

Cluster role	Capabilities
	<ul style="list-style-type: none"> • Performing SnapLock operations, including privileged delete • Configuring protocols: NFS and SMB • Configuring services: DNS, LDAP, and NIS • Monitoring jobs • Monitoring network connections and network interface
vsadmin-readonly	<ul style="list-style-type: none"> • Managing own user account local password and key information • Monitoring the health of the SVM • Monitoring network interface • Viewing volumes and LUNs • Viewing services and protocols

See below for an example of creating a read-only user for monitoring the health of the storage cluster using ssh application with password authentication. The command prompts for a password and password confirmation.

```
SiteA::> security login create -vserver SiteA -user-or-group-name fpmonitor -application ssh -
authentication-method password -role readonly
```

```
Please enter a password for user 'fpmonitor':
Please enter it again:
```

In addition to using RBAC for access control and privileges management, beginning with ONTAP 9.11.1, you can use multi-admin verification (MAV) to ensure that certain protected operations, such as deleting volumes or Snapshot[®] copies, can be executed only after approvals from designated administrators. Please see Appendix B: ONTAP multi-admin verification example for MAV configuration and usage information.

VMware vSphere role-based access control

In VMware vCenter Server, system roles and sample roles are provided by default, and you can also create custom roles. A role is a predefined set of privileges for rights to perform actions and read properties. Permissions are created by assigning a role and its associated privileges to a user or group for an object.

See Table 9 for information on the predefined vCenter Server roles. To meet the needs of your environment, you can create custom roles by cloning an existing role and modifying the cloned copy for your environment.

Table 9) Predefined vCenter Server roles and description.

Role type	Role names	Description
System	Administrator, Read-only, No access	The system roles are organized as a hierarchy. Each role inherits the privileges of the previous role. System roles are permanent, and you cannot delete system roles nor edit their privileges.
Sample	Examples: AutoUpdateUser, Resource pool administrator, and Virtual machine user.	The sample roles are provided for certain frequently performed combination of tasks. You can clone, modify, or remove these roles.

Since privileges provide fine-grained access controls in vSphere, it can be difficult to determine the minimum set of privileges that are required to perform a set of operations. Implemented with REST API,

the vSphere privilege recorder feature can help you identify the minimum set of required privileges to run a certain vCenter Server workflow.

Table 10 shows the vCenter local user roles and capabilities. To create a local user account in vCenter Server, log in to vCenter Server appliance shell as root and run the command as shown in the example below to add a local user and list the local users. You can optionally provide full name and email address information when adding a user.

```
Command> localaccounts.user.add --role operator --username fpmonitor --password
Enter password:
Reenter password:

Command> localaccounts.user.list
Config:
  1:
    Username: root
    Role: superAdmin
    Fullname: root
    Status: enabled
    Passwordstatus: never_expire
    Email: ''
  2:
    Username: fpmonitor
    Role: operator
    Fullname: fpmonitor
    Status: enabled
    Passwordstatus: valid
    Email: ''
```

Table 10) vCenter Server local user roles and capabilities.

Role name	Capabilities
Operator	Read vCenter Server configuration
Administrator	Configure vCenter Server
Super Administrator	Configure vCenter Server, manage local account, and use the Bash shell

Login banners

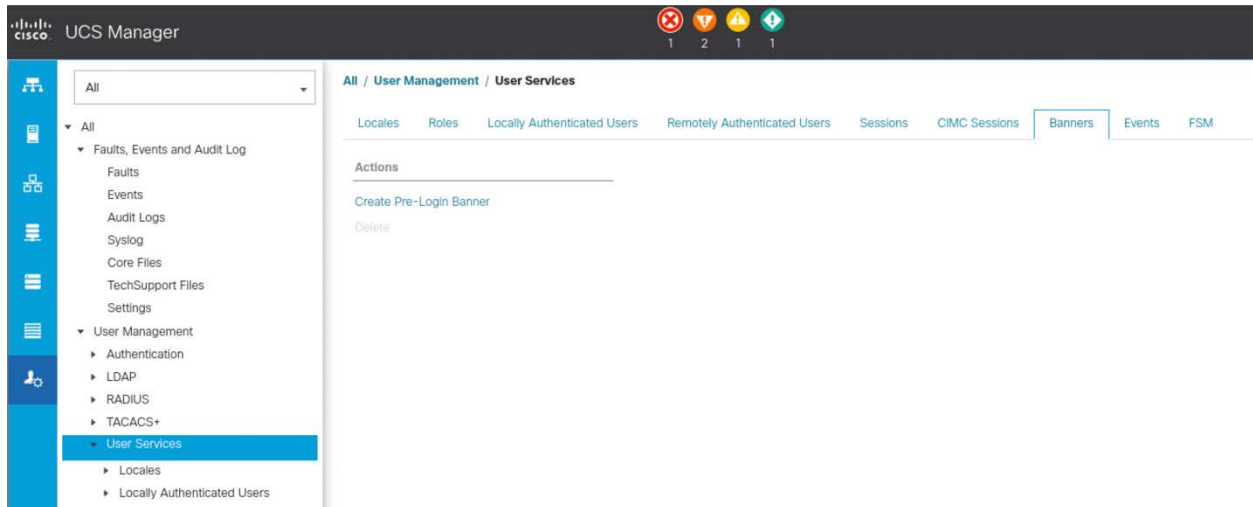
Login banners allow an organization to present any operators, administrators, and even miscreants with terms and conditions of acceptable use, and they indicate who is permitted access to the system. This approach is helpful for establishing expectations for access and use of the system.

How the banners are configured varies between the FlexPod components. For this security hardening efforts, we are focusing on the banner message which shows up during authentication when a user tries to connect to the device and before the user is presented with the password prompt.

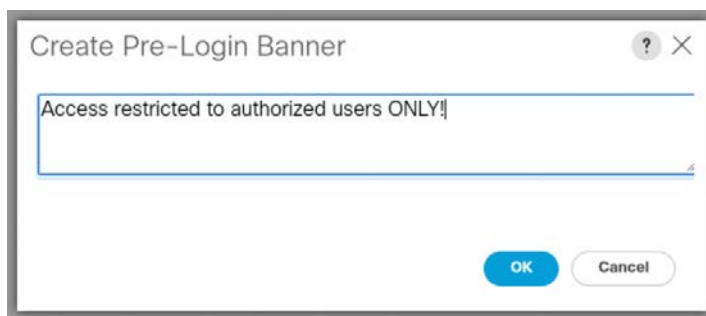
Cisco UCS Manager login banners

UCS Manager supports the creation of the Pre-Login Banner. To create the banner, login to UCS Manager and perform the following steps.

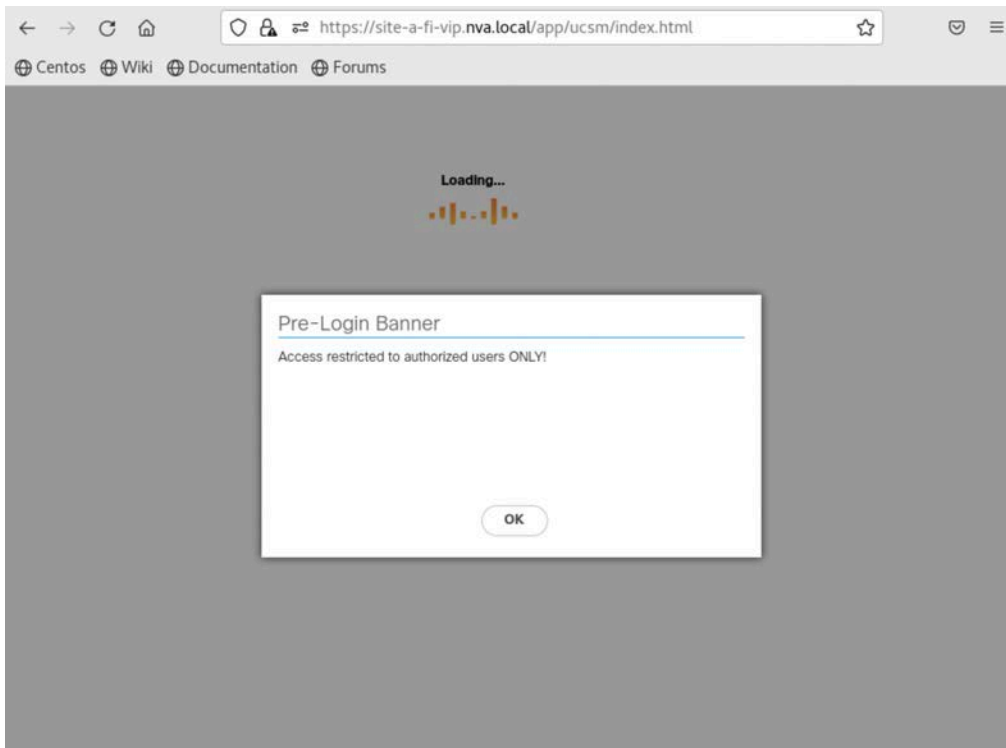
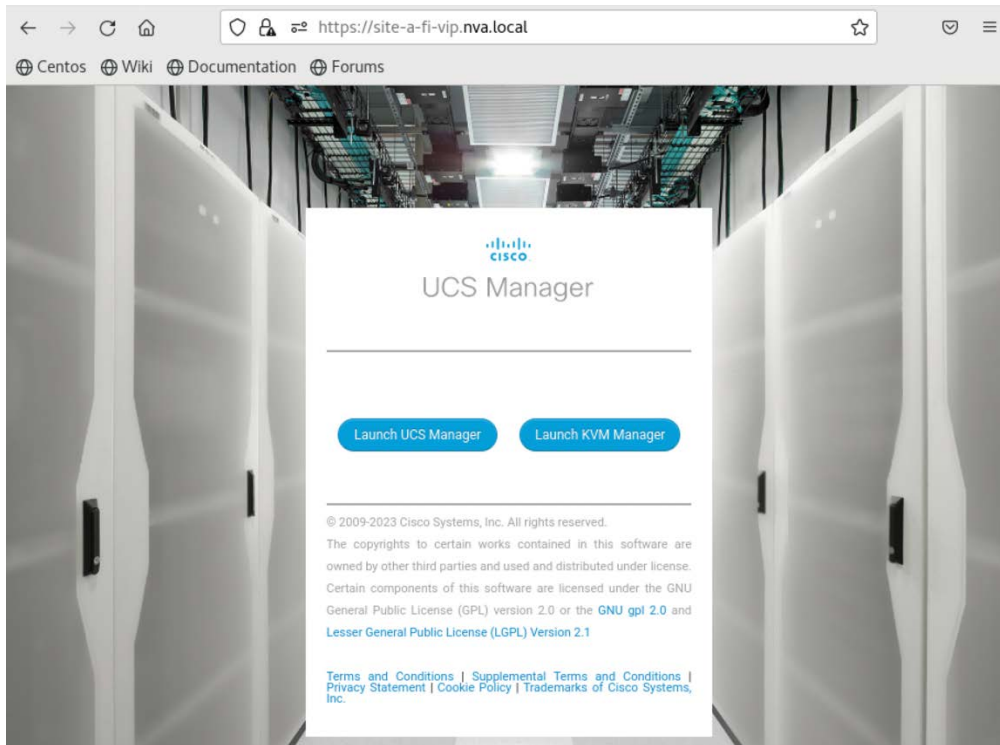
Click the Admin tab in the Navigation pane, expand All > User Management, click the Banners tab in the Work pane, click Create Pre-Login Banner Action.



In the Create Pre-Login Banner dialog box, click in the text field and enter the message for the user to see before they login to Cisco UCS Manager. Click OK when done and click OK again on the successful creation of the banner.



Logout of UCS Manager and launch a new browser window to connect to the UCS Manager web page. After selecting Launch UCS Manager, the pre-login banner is presented to the user. After acknowledging the pre-login banner, user can then provide the login credentials.



When accessing the UCS Manager via CLI, the pre-login banner is presented before the password prompt as seen in the example below.

```
$ ssh admin@site-a-fi-vip.nva.local
Access restricted to authorized users ONLY!
```

```
admin@site-a-fi-vip.nva.local's password:
```

Cisco Nexus login banners

On the Cisco Nexus 9k switches, you can configure message-of-the-day (MOTD) banner to display a login banner during authentication process before the password prompt is presented to the user. The MOTD banner can be up to 40 lines and up to 80 characters per line.

To create MOTD banner, enter global configuration mode, invoke the `banner motd` command and provide the banner message inline. In the following example, (#) is used as the message delimiter. After receiving a line feed character, the (>) prompt is displayed. Repeat the delimiter (#) to complete the message for the command.

```
SiteA-switch-a.nva.local# conf terminal
Enter configuration commands, one per line. End with CNTL/Z.

SiteA-switch-a.nva.local(config)# banner motd #Access restricted to authorized users ONLY!
> #

SiteA-switch-a.nva.local(config)# exit

SiteA-switch-a.nva.local# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.

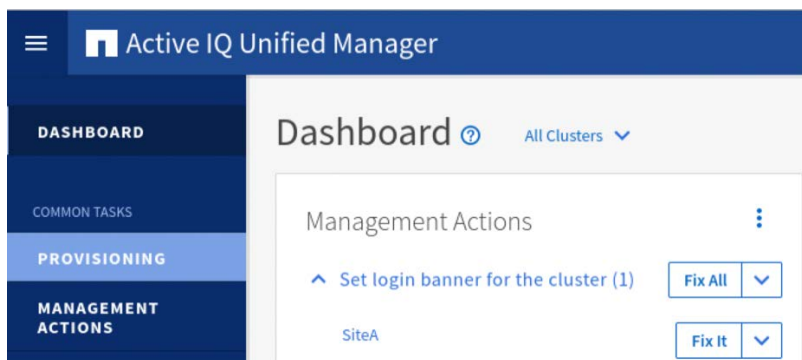
SiteA-switch-a.nva.local# exit
Connection to sitea-switch-a.nva.local closed.
```

After the MOTD banner is created, logout and then login again to check the banner message.

```
$ ssh admin@SiteA-switch-a.nva.local
Access restricted to authorized users ONLY!
Password:
```

NetApp ONTAP login banners

NetApp Active IQ Unified Manager (AIQUM) checks for the presence of the cluster login banner. If a login banner has not been configured in the cluster, AIQUM reports it as a management action on its Dashboard as shown in the screenshot below.



The Fix it button on the AIQUM Dashboard can be used to automatically configure the cluster with a login banner of “Access restricted to authorized users”.

Alternatively, the ONTAP `security login banner modify` command can be used to manually modify the login banner. The banner text must be in double quotes (“ ”), as shown in the following example.

```
SiteA::~> security login banner modify -vserver SiteA -message "Access restricted to authorized users ONLY!"
```

The login banner is displayed just before the authentication step during the SSH and console device login process.

```
$ ssh admin@SiteA.nva.local
Access restricted to authorized users ONLY!
Password:
```

A login banner can also be created for a storage virtual machine (SVM). The follow lists how the cluster-level and SVM-level login banners interact.

- The banner configured for the cluster is also used for all SVMs that do not have a banner message defined.
- An SVM-level banner can be configured for each SVM.
- If a cluster-level banner has been configured, it is overridden by the SVM-level banner for the given SVM.

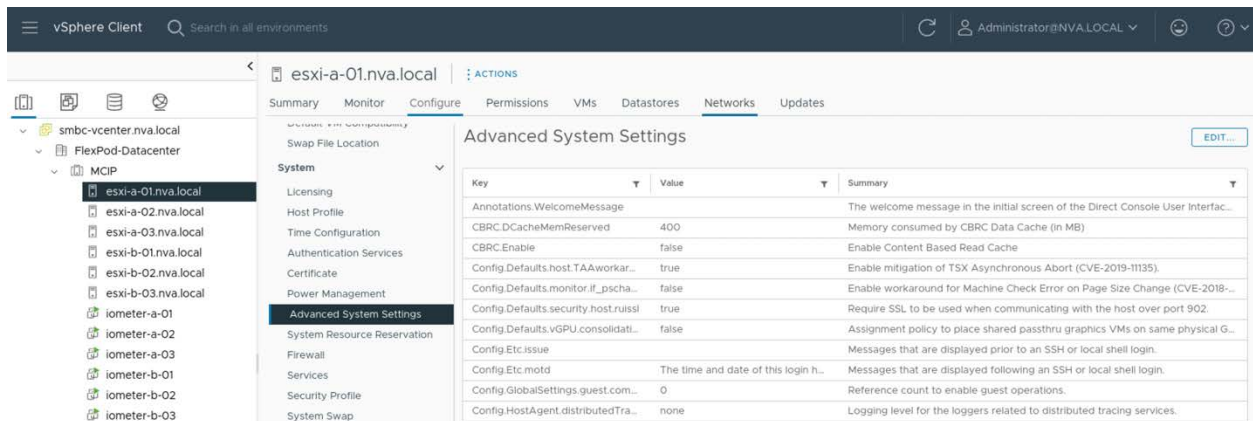
In addition to the login banner, you can also create a cluster-level and/or an SVM-level message of the day (MOTD) banner to communicate information to the users after login. Please see the `security login motd modify` command in ONTAP documentation for details on its configuration.

VMware vSphere login banners

ESXi login banners

For VMware ESXi hosts, you can create a login banner by log in to the vCenter Server with the vSphere Client and perform the following steps.

Select the ESXi host in the inventory, click the Configure tab, and select the Advanced System Settings under System.



Click the Edit icon, enter a login message in the value field of the Annotations.WelcomeMessage key, and click Ok.

Edit Advanced System Settings | esxi-a-01.nva.local



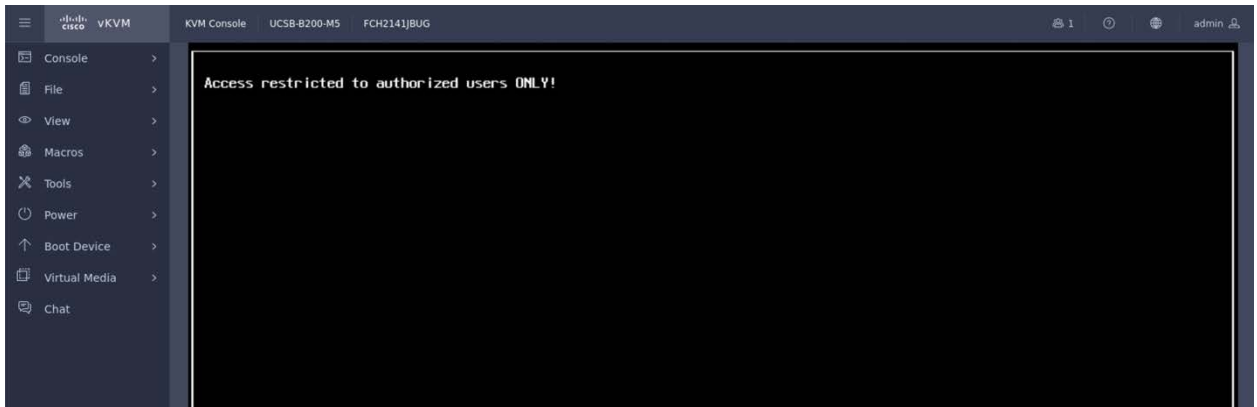
Modifying configuration parameters is unsupported and can cause instability. Continue only if you know what you are doing.

Key	Value
Annotations.WelcomeMessage	<u>Access restricted to authorized users ONLY</u>
CBRC.DCacheMemReserved	400
CBRC.Enable	false
Config.Defaults.host.TAAworkaround	true
Config.Defaults.monitor.if_pschange_mc_workaround	false
Config.Defaults.security.host.ruissl	true
Config.Defaults.vGPU.consolidation	false
Config.Etc.issue	
Config.Etc.motd	The time and date of this login have been sent to the system
Config.GlobalSettings.guest.commands.sharedPolicyRefCour	0
Config.HostAgent.distributedTracing	none
Config.HostAgent.level[Hbrsvc].logLevel	
Config.HostAgent.level[Hostsvc].logLevel	
Config.HostAgent.level[Proxysvc].logLevel	
Config.HostAgent.level[Snmpsvc].logLevel	
Config.HostAgent.level[Statssvc].logLevel	
Config.HostAgent.level[Vcsvc].logLevel	
Config.HostAgent.level[Vimsvc].logLevel	

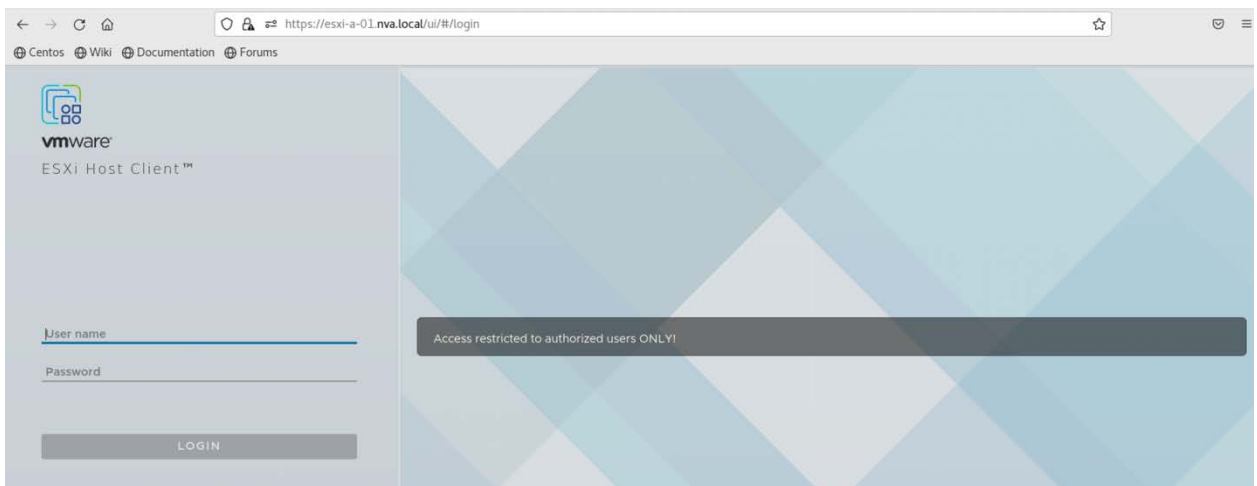
CANCEL

OK

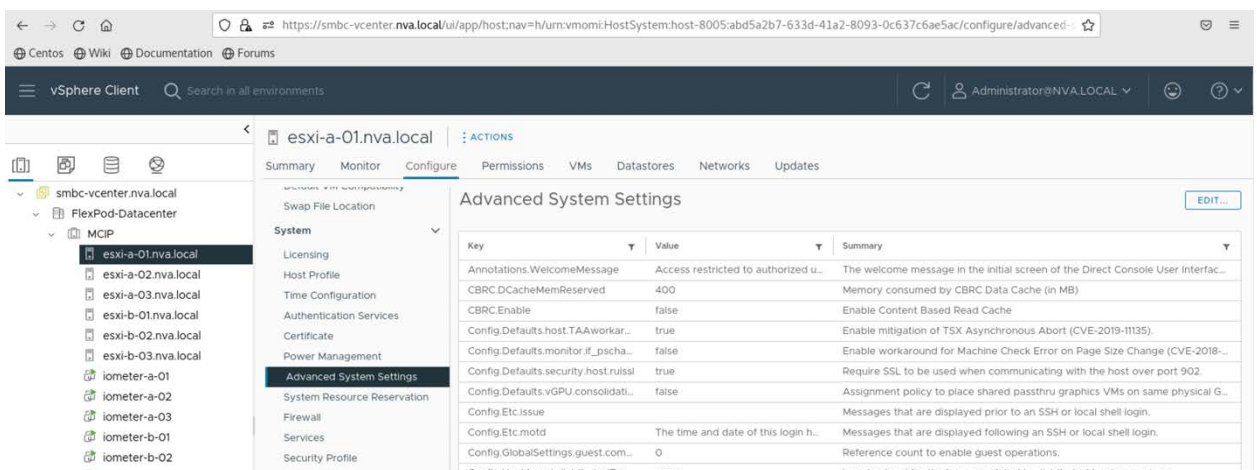
Log in to UCS Manager, select the Service Profile associated with the ESXi host under Servers and launch the associated KVM console to check the login banner on the direct console of the ESXi host.



Open a web browser and connect to the VMware Host Client to check the login banner on the VMware Host Client login screen.



For the ssh login banner, provide the banner message as value to the Config.Etc.issue key in the Advanced System Settings.



 Modifying configuration parameters is unsupported and can cause instability. Continue only if you know what you are doing.

Key	Value
Annotations.WelcomeMessage	Access restricted to authorized users ONLY!
CBRC.DCacheMemReserved	400
CBRC.Enable	false
Config.Defaults.host.TAAworkaround	true
Config.Defaults.monitor.if_pschange_mc_workaround	false
Config.Defaults.security.host.ruissl	true
Config.Defaults.vGPU.consolidation	false
Config.Etc.issue	Access restricted to authorized users ONLY!
Config.Etc.motd	The time and date of this login have been sent to the system
Config.GlobalSettings.guest.commands.sharedPolicyRefCour	0
Config.HostAgent.distributedTracing	none
Config.HostAgent.level[Hbrsvc].logLevel	
Config.HostAgent.level[Hostsvc].logLevel	
Config.HostAgent.level[Proxysvc].logLevel	
Config.HostAgent.level[Snmpsvc].logLevel	
Config.HostAgent.level[Statssvc].logLevel	
Config.HostAgent.level[Vcsvc].logLevel	
Config.HostAgent.level[Vimsvc].logLevel	

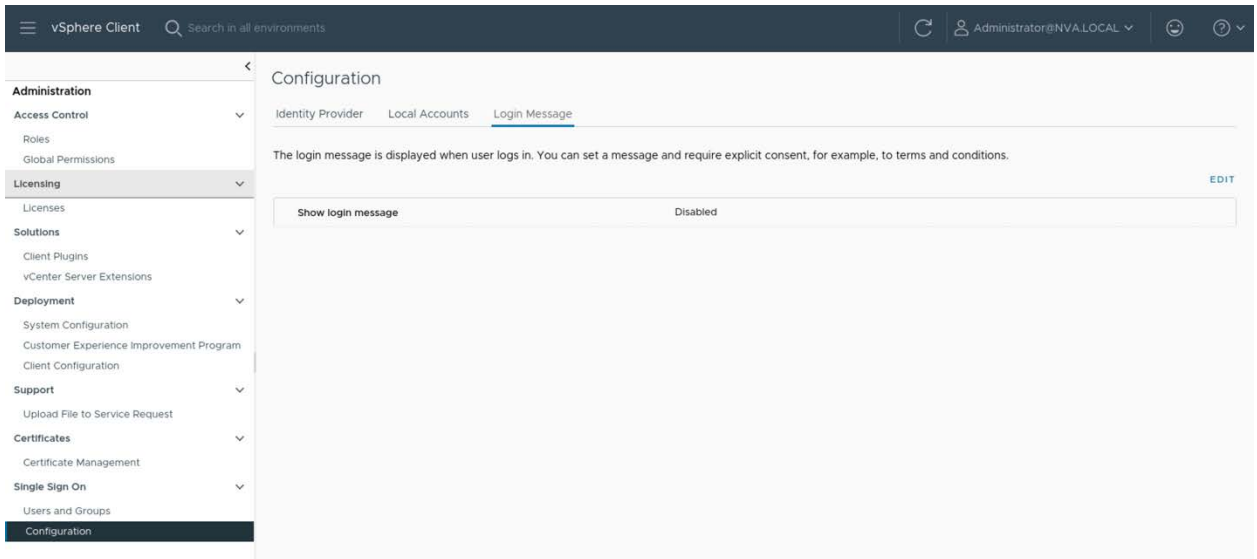
CANCEL

OK

vCenter Server login banner

To create a login banner for vCenter Server, log in to vCenter Server with vSphere Client and perform the following steps.

Select Administration from the Home menu, click Configure under Single Sign On, click Login Message tab, and then click Edit to configure the login message.



Toggle on Show login message to enable login message, provide a Title for the Login message, toggle on Consent checkbox to require user consent, provide the Details of the login message, and click Save.

Edit login message

×

Show login message

☒

▼ Login message

I agree to Restricted Access

Consent checkbox

☒

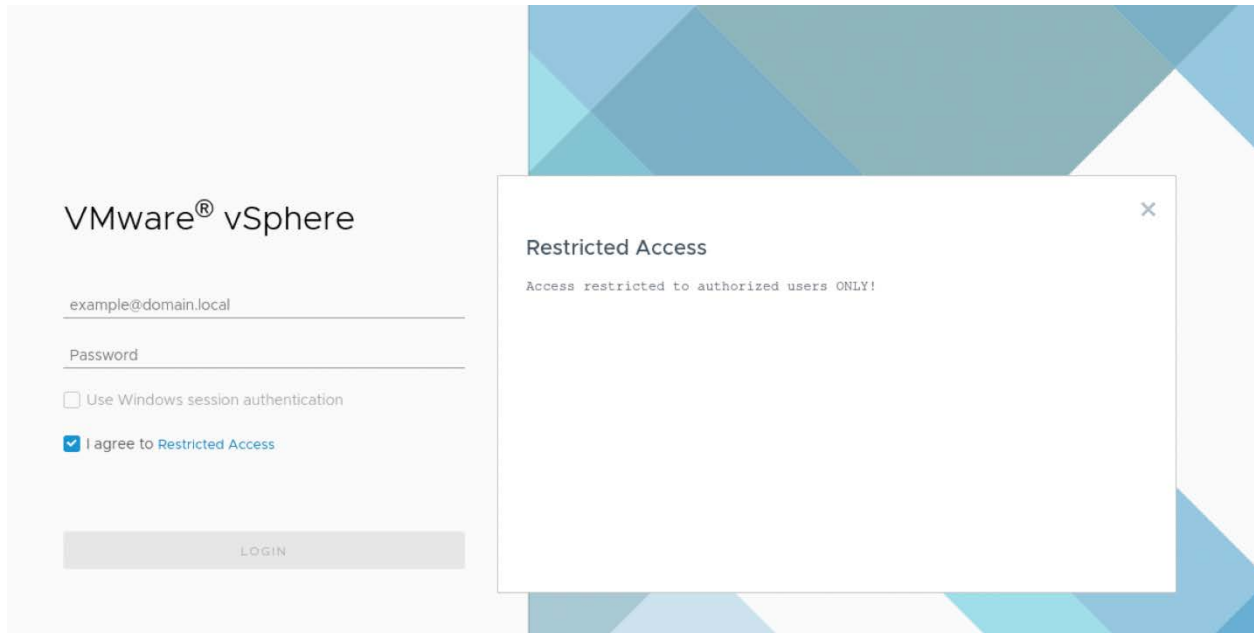
Details of login message

Access restricted to authorized users ONLY!

CANCEL

SAVE

Log out of vCenter Server to check the updated login banner. In this example, user needs to provide consent in addition to providing login credentials to login. The detail message is provided when user clicks on the message title, Restricted Access.



Login session timeout and limits

The login session timeout and limits are important to prevent stale sessions and session piggybacking and to reduce attack surfaces.

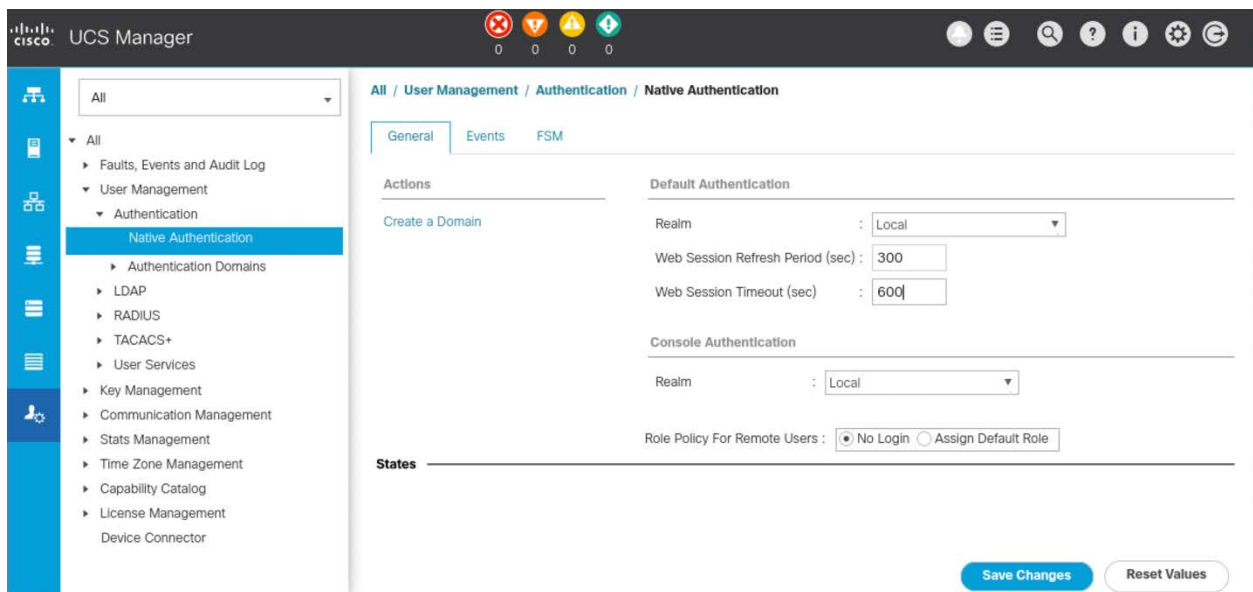
Cisco UCS Manager login session timeout and limits

UCS Manager web session refresh request and timeout

When a web client connects to UCS Manager, the client must send refresh requests to UCS Manager to keep the web session active. The Refresh Period option specifies the maximum amount of time allowed between web client refresh requests for a user. The Session Timeout option specifies the maximum amount of time that can elapse after the last refresh request has failed before UCS Manager considers a web session as inactive. The default UCS Manager web session Refresh Period is 600 seconds, and the default Session Timeout is 7200 seconds.

To change the web session Refresh Period and Session Timeout options, click Admin tab in the UCS Manager Navigation pane, expand All > User Management > Authentication. Click Native Authentication, update the web session options in the General tab Default Authentication area, click Save Changes, and then click Ok.

The following example shows setting the Web Session Refresh Period to 300 seconds and Web Session Timeout to 600 seconds.

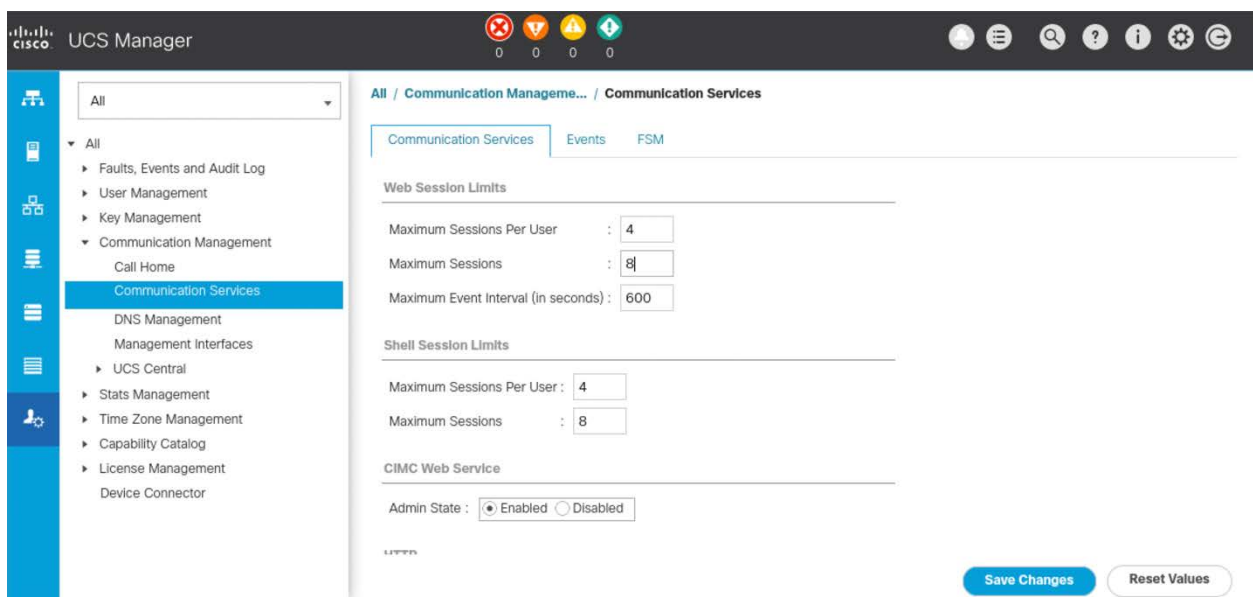


UCS Manager web session and shell session limits

At any given time, UCS Manager restricts the number of web sessions that a given user is permitted to access and the total number of web sessions permitted from all users. Each UCS Manager domain supports a default of maximum of 32 concurrent web sessions per user and 256 total user web sessions. The supported default shell session per user and maximum shell sessions are both 32.

To change web session and shell session limits, navigate to Admin > Communication Management > Communication Services, update the maximum per user session and maximum total sessions, click Save Changes, and then click Ok.

The following shows an example of setting the maximum to 4 web sessions per user, 8 total web sessions, 4 shell sessions per user, and 8 total shell sessions.



Cisco Nexus login session timeout and limits

On Cisco Nexus switches, the default inactive session timeout is 30 minutes, and the default session limit is 32. The following is an example of entering global configuration mode, updating the inactive session timeout to 15 minutes, reducing the session limit to 4, saving the configuration, and then checking for those updated settings.

```
SiteA-switch-a.nva.local# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SiteA-switch-a.nva.local(config)# line vty
SiteA-switch-a.nva.local(config-line)# exec-timeout 15
SiteA-switch-a.nva.local(config-line)# session-limit 4
SiteA-switch-a.nva.local(config-line)# exit
SiteA-switch-a.nva.local(config)# exit

SiteA-switch-a.nva.local# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.

SiteA-switch-a.nva.local# show running-config all | begin vty
line vty
  session-limit 4
  exec-timeout 15
  logout-warning 20
  absolute-timeout 0
...
```

NetApp ONTAP login session timeout and limits

The default ONTAP CLI session timeout is 30 minutes. To see the session timeout setting or to modify the timeout setting, invoke the `system timeout` commands as shown in the example below.

```
SiteA::> system timeout show
CLI session timeout: 30 minutes

SiteA::> system timeout modify -timeout 15

SiteA::> system timeout show
CLI session timeout: 15 minutes
```

The ONTAP management session limits can also be modified based on the access interfaces (`cli` / `ontapi` / `rest`) and categories (`application` / `location` / `request` / `vserver`). The following example demonstrates how to show the default management session limits, modify the defaults for the maximum active CLI sessions, and show the updated settings.

```
SiteA::> security session limit show
Interface Category      Max-Active
-----
cli          application      64
cli          location         32
cli          vserver           16
ontapi       application      20
ontapi       location         20
ontapi       request          20
ontapi       vserver           10
rest         application      20
rest         location         20
rest         request          20
rest         vserver           10
11 entries were displayed.

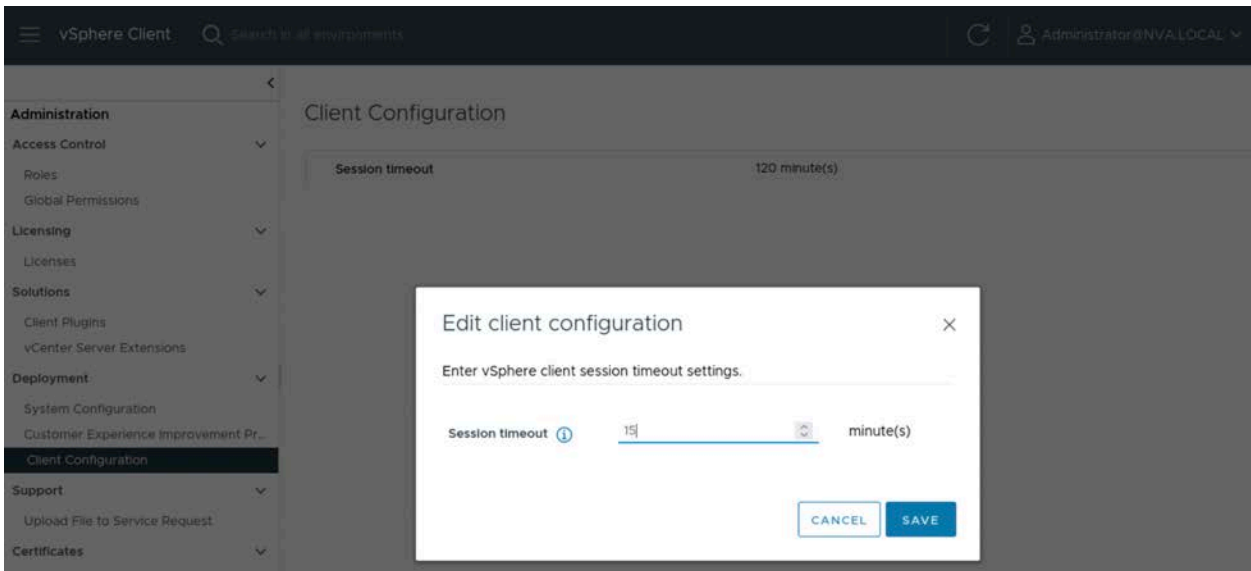
SiteA::> security session limit modify -interface cli -category * -max-active-limit 4
3 entries were modified.

SiteA::> security session limit show
```

Interface	Category	Max-Active
cli	application	4
cli	location	4
cli	vserver	4
ontapi	application	20
ontapi	location	20
ontapi	request	20
ontapi	vserver	10
rest	application	20
rest	location	20
rest	request	20
rest	vserver	10
11 entries were displayed.		

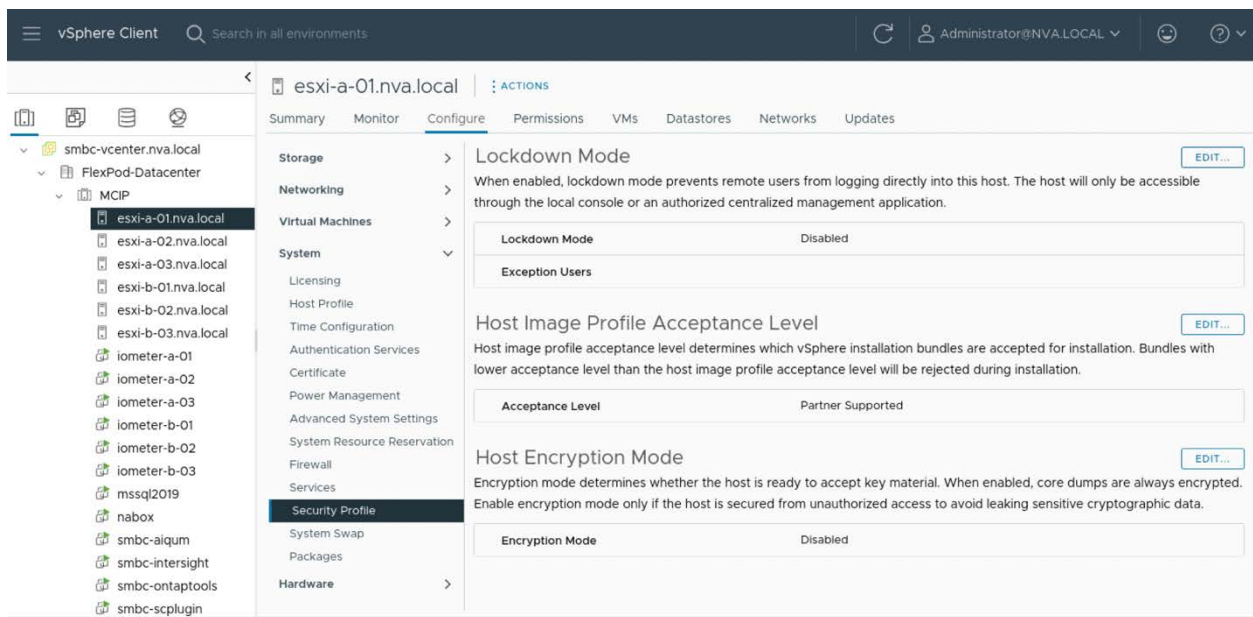
VMware vSphere login session timeout and limits

The default vSphere Client login session timeout is 120 minutes. To change the setting, log into vSphere Client, go to Home > Administration > Deployment > Client Configuration, click Edit and update the setting in the Edit client configuration dialog as shown in the example below, and then click Save.



For the vSphere hosts managed by a vCenter Server, you can enable Lockdown Mode for the hosts. When the Normal Lockdown Mode is enabled for a host, the host is only accessible through the local console or the vCenter Server. When the Strict Lockdown Mode is enabled for a host, the host is only accessible through the vCenter Server.

To enable Lockdown mode, log into vCenter Server, select a host, go to Configure > System > Security Profile, click Edit for Lockdown Mode and select the desired lockdown mode as shown in the examples below, and then click Ok.



esxi-a-01.nva.local - Lockdown Mode



Lockdown Mode

Exception Users

Lockdown Mode

When enabled, lockdown mode prevents remote users from logging directly to this host. The host is accessible only through the local console or vCenter Server.

Specify host lockdown mode:

☐ Disabled

Lockdown mode is disabled.

☒ Normal

The host is accessible only through the local console or vCenter Server.

☐ Strict

The host is accessible only through vCenter Server. The Direct Console UI service is stopped.

CANCEL

OK

Time synchronization

The network time protocol (NTP) is used to synchronize the time between FlexPod components. Inadequate time synchronization makes troubleshooting issue logs from the various solution components of the FlexPod solution challenging.

For a clustered solution like the ONTAP storage cluster, problems can occur when the time on the nodes are not accurately synchronized. As a result, it is a best practice to configure and use NTP servers to synchronize the time of the FlexPod components.

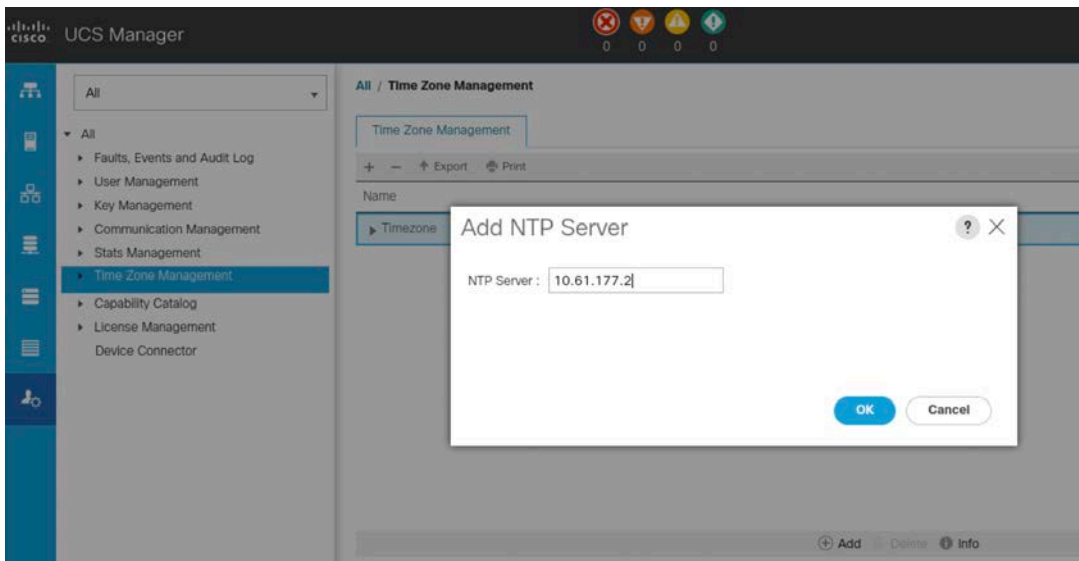
Precision Time Protocol (PTP) is defined in IEEE 1588 to improve the clock synchronization of network measurements and control systems. While the accuracy expectations of NTP ranges from a few microseconds to tens of milliseconds depending on the environment, the accuracy expectation of PTP is in the order of 100 nanoseconds depending on the resolution and accuracy of the hardware. The improved timing precision enhances network monitoring accuracy and troubleshooting ability.

PTP is supported on Cisco Nexus and on vSphere ESXi hosts. However, Cisco UCS Manager, NetApp ONTAP, and VMware vCenter Server currently support NTP for time synchronization. The following sections discuss utilizing NTP for time synchronization of the FlexPod components.

Cisco UCS Manager time synchronization

For Cisco UCS Manager to display the time correctly, it requires a domain-specific time zone and an NTP server. Use the following steps to configure the time zone and NTP server settings in UCS Manager.

To configure NTP server in the UCS Manager, click the Admin tab in the Navigation pane, expand All in the Admin tab, click Time Zone Management, click Timezone, click Add, enter NTP server information in the pop-up Add NTP Server dialog, click Ok, and then click Ok again.



With Timezone still selected under Time Zone Management, click info to enter Properties for Timezone dialog, use the dropdown list under Properties to select the appropriate time zone, click Apply, then click Ok on the Success message. You can use the Add NTP Server Action in the Properties for Timezone dialog to add additional NTP servers.

Properties for: Timezone ✕

General Events

Actions

Add NTP Server

Properties

Time Zone : ca/New_York (Eastern Time) ▼

NTP Servers

Advanced Filter
Export
Print

Name

NTP Server 10.61.177.2

Add
Delete
Info

OK

Apply

Cancel

Help

Cisco Nexus time synchronization

NTP client

You can configure the Cisco NX-OS switch to synchronize time with an external NTP server during the initial device initialization. You also have the option to configure it from the global configuration mode and check the configuration as the following example shows.

```
SiteA-switch-a.nva.local# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SiteA-switch-a.nva.local(config)# ntp server 10.61.177.2 use-vrf management
SiteA-switch-a.nva.local(config)# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
SiteA-switch-a.nva.local(config)# exit

SiteA-switch-a.nva.local# show ntp peers
-----
Peer IP Address          Serv/Peer
-----
10.61.177.2              Server (configured)
```

NTP distribution

The Cisco NX-OS device can use NTP to distribute time, so other devices can use it as a time server. It can also act as an authoritative NTP server to distribute time to other devices even when it is not synchronized to an outside time source.

FlexPod CVDs and NVAs typically configures the FlexPod switches to distribute time for in-band management (IB-MGMT) network. The following is an example for configuring two NX-OS switches as NTP peers for the IB-MGMT network time distribution.

Switch A:

```
SiteA-switch-a.nva.local# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SiteA-switch-a.nva.local(config)# interface vlan3334
SiteA-switch-a.nva.local(config-if)# ip address 172.21.78.121/24
SiteA-switch-a.nva.local(config-if)# no shutdown
```

```

SiteA-switch-a.nva.local(config-if)# exit
SiteA-switch-a.nva.local(config)# ntp peer 172.21.77.122 use-vrf management
SiteA-switch-a.nva.local(config)# exit
SiteA-switch-a.nva.local# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.

```

Switch B:

```

SiteA-switch-b.nva.local# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SiteA-switch-b.nva.local(config)# interface vlan3334
SiteA-switch-b.nva.local(config-if)# ip address 172.21.78.122/24
SiteA-switch-b.nva.local(config-if)# no shutdown
SiteA-switch-b.nva.local(config-if)# exit
SiteA-switch-b.nva.local(config)# ntp peer 172.21.77.121 use-vrf management
SiteA-switch-b.nva.local(config)# exit
SiteA-switch-b.nva.local# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.

```

Note: The IB-MGMT VLAN in the example is VLAN 3334. The IB-MGMT network NTP IPs for switch A and B are 172.21.78.121 and 172.21.78.122, respectively. The management IPs for switch A and B are 172.21.77.121 and 172.21.77.122, respectively.

NetApp ONTAP time synchronization

Although ONTAP enables you to manually set the time zone, date, and time on the cluster, you must configure the Network Time Protocol (NTP) servers to synchronize the cluster time with external NTP servers.

You can associate a maximum of 10 external NTP servers by using the `cluster time-service ntp server create` command. For redundancy and quality of time service, you should associate at least three external NTP servers with the cluster.

Please see below for an example of using CLI to add two additional external NTP servers to ONTAP cluster time service when there is one NTP server already configured.

```

SiteA::> cluster time-service ntp server show
              Is
              Authentication
Server        Version  Enabled    Key ID
-----
10.61.177.2   auto    false     -

SiteA::> cluster time-service ntp server create -server 10.61.176.251

SiteA::> cluster time-service ntp server create -server 10.61.176.252

SiteA::> cluster time-service ntp server show
              Is
              Authentication
Server        Version  Enabled    Key ID
-----
10.61.176.251 auto    false     -
10.61.176.252 auto    false     -
10.61.177.2   auto    false     -
3 entries were displayed.

```

To update the NTP server configuration with the ONTAP System Manager, perform the following steps.

Log in to ONTAP System GUI as administrator user, select CLUSTER > Overview, click More on the right-hand side to show the additional options, select Edit, click +Add under NTP SERVERS, provide the NTP server IP information and press Enter. Click Save when done with adding NTP servers.

ONTAP System Manager

Search actions, objects, and pages

DASHBOARD

INSIGHTS

STORAGE

NETWORK

EVENTS & JOBS

PROTECTION

HOSTS

CLUSTER

Overview

Hardware

Settings

Overview

Overview

NAME

SiteA

VERSION

NetApp Release 9.13.1P1: Tue Jul 25 10:19:28 UTC 2023

UUID

7d0400a8-3cde-11ed-ae78-00a098dcc6b6

LOCATION

"RTP/Lab1"

NTP SERVERS

10.61.177.2

DNS DOMAINS

nva.local

NAME SERVERS

10.61.177.2

MANAGEMENT INTERFACES

172.21.77.100

DATE AND TIME

September 11, 2023, 3:52 PM America/New_York

More

ONTAP Update

Rename

Edit

Login Banner Message

Download Configuration

Edit Cluster Details

NAME

SiteA

LOCATION

"RTP/Lab1"

DNS DOMAINS

nva.local

+ Add

NAME SERVERS

10.61.177.2

+ Add

NTP SERVERS

10.61.177.2

10.61.176.251

10.61.176.252

+ Add

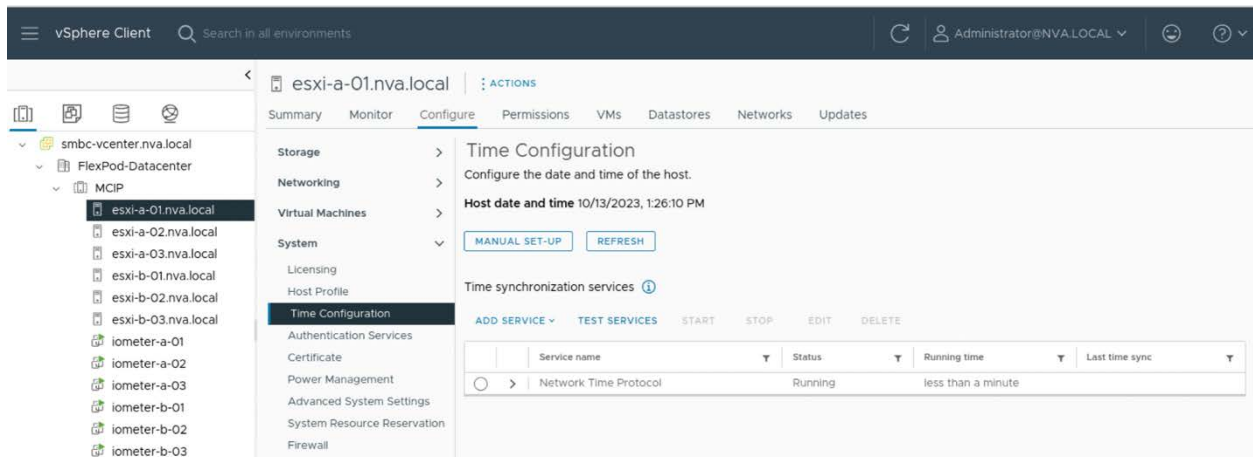
☐ Add cluster management interface

Save

Cancel

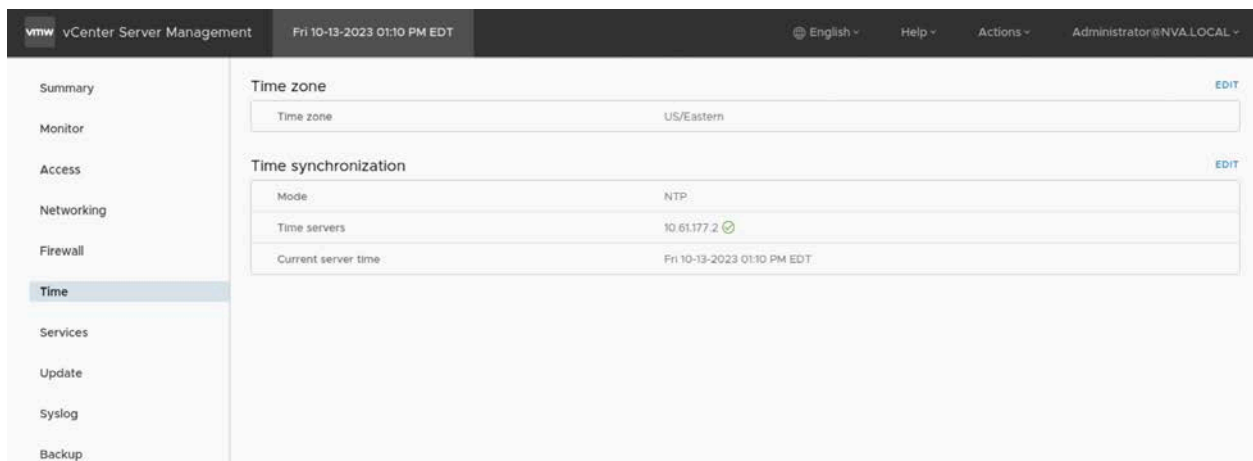
VMware vSphere time synchronization

You can configure NTP on ESXi hosts using the vSphere Web Client by following the steps below. Log in to the vCenter Server, select Hosts and Clusters, select an ESXi host, navigate to the Configure tab, select Time Configuration under System and click Edit. Then, select Network Time Protocol under the Add Service menu, enter the NTP Server(s) you want to use and click Ok. Select the service and click Start to start the service if its status is Stopped.



For vCenter Server, you can configure its time settings to synchronize with the ESXi host on which vCenter Server is running or with an external NTP server. The time zone and time settings can be configured in the appliance by using the following steps.

Log in to the vCenter Server Management Interface as root and select Time in the management interface. To set the time zone, click Edit in the Time Zone pane, select the appropriate time zone from the drop-down list, and click Save. To set the NTP servers, click Edit in the Time Synchronization pane, select NTP from the Mode drop-down list, enter the NTP servers in the dialog box, and click Save.



Remote logging

Prior to setting up remote logging on the FlexPod components, a remote syslog server must already exist. If your environment does not already contain a syslog server, you must first create one. If your environment already contains a syslog server for logging events from other systems, then you might want to use that one for important event notifications as well.

Cisco UCS Manager remote logging

Cisco UCS Manager generates log messages to record routine system operations, failures and errors, and critical and emergency conditions. To send the log messages to external syslog servers, log in to Cisco UCS Manager GUI and perform the following steps.

Click Admin in the Navigation pane, expand All > Faults, Events, and Audit Log, and click Syslog. Enable RFC 5424 format syslog message if desirable.

Then, under the Remote Destinations Server 1 area, select Enabled for Admin State, select the lowest message level to save, provide the hostname or IP of the syslog server, and select a Facility.

Under the Local Sources area, configure Admin States for Faults, Audits, and Events to Enabled to log all system faults, audit log events, and system events.

Click on Save Changes at the bottom of the page to commit and then click Ok on the Success message.

The screenshot shows the Cisco UCS Manager interface for configuring Syslog. The left sidebar contains a navigation menu with options like All, Faults, Events and Audit Log, Syslog, Core Files, TechSupport Files, Settings, User Management, Authentication, LDAP, RADIUS, TACACS+, User Services, Locales, Locally Authenticated Users, Login Profile, Remotely Authenticated Users, Roles, Key Management, KeyRing default, Communication Management, Call Home, Communication Services, DNS Management, Management Interfaces, UCS Central, State Management, Collection Policies, Collection Policy Chassis, and Collection Policy Fax. The main content area is titled 'All / Faults, Events and Audit Log / Syslog'. It includes sections for Global Settings (RFC 5424 Compliance: Enabled/Disabled), Local Destinations (Console, Monitor, File), Remote Destinations (Server 1, Server 2, Server 3), and Local Sources (Faults, Audits, Events). The Syslog tab is active. Under Remote Destinations Server 1, the Admin State is set to Enabled, the Level is 'warnings (UCSM Minor)', the Hostname (or IP Address) is 'control.nva.local', and the Facility is 'Local7'. Under Local Sources, the Admin State is set to Enabled for Faults, Audits, and Events. At the bottom right, there are 'Save Changes' and 'Reset Values' buttons.

Cisco Nexus remote logging

System message logging controls the destination and filters the severity level of messages that system processes generate. By default, the device outputs messages to terminal sessions and logs system messages to a log file. You can also configure logging to syslog servers on remote systems.

Cisco recommends configuring the syslog server to use the management virtual routing and forwarding (VRF) instance. You can configure up to eight syslog servers to log system messages remotely.

The following is an example for configuring a remote syslog server for logging messages using the management VRF.

```
SiteA-switch-a.nva.local# conf terminal
Enter configuration commands, one per line. End with CNTL/Z.

SiteA-switch-a.nva.local(config)# logging server 10.61.177.2 5 use-vrf management

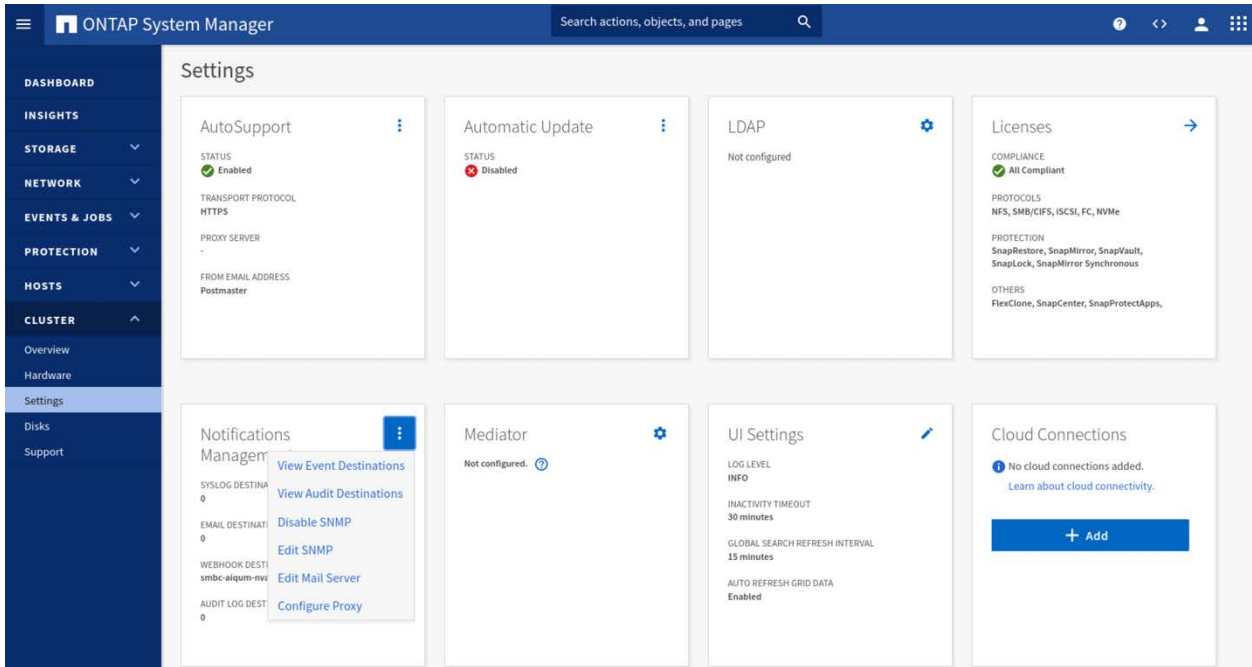
SiteA-switch-a.nva.local(config)# show logging server
Logging server:                enabled
{10.61.177.2}
  server severity:              notifications
  server facility:              local7
  server VRF:                   management
  server port:                  514

SiteA-switch-a.nva.local(config)# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
```

NetApp ONTAP remote logging

You can configure the ONTAP Event Management System (EMS) to forward notifications for events to a syslog server. Perform the following steps in ONTAP System Manager to configure syslog server information.

Click Cluster > Settings, then click the ellipses in the Notifications Management section and select View Event Destinations.



Select Events Destinations tab on the Notification Management page, click +Add to add a new destination.

In the Add event destination dialog, provide a name for the destination, select Forward to a syslog server, and enter the syslog server hostname or IP, syslog port, and syslog transport.

Add event destination

NAME

EMS-syslog

DESTINATION TYPE

☐ Email

☒ Forward to a syslog server

HOST NAME OR IP ADDRESS

control.nva.local

SYSLOG PORT

514

SYSLOG TRANSPORT

TCP Unencrypted

☐ Webhook [?](#)

EVENT FILTERS

Select Event Filters

[Add a new event filter](#)

Save

Cancel

In the EVENT FILTERS field, click Select Event Filters to select an existing event filter, such as the one from Active IQ Unified Manager, or select Add a new event filter below it. Click Save when done and check the Event Destinations tab to confirm the created syslog destination.

Add event destination

NAME

EMS-syslog

DESTINATION TYPE

☐ Email

☒ Forward to a syslog server

HOST NAME OR IP ADDRESS

control.nva.local

☐ default-trap-events
4 rules

☐ important-events
3 rules

☐ no-info-debug-events
2 rules

☒ smbc-aicum-nva-local_filter
32 rules

smbc-aicum-nva-lo... X |

[Add a new event filter](#)

Save Cancel

ONTAP System Manager

Search actions, objects, and pages

Notifications Management Cluster Settings

Event Destinations Audit Log Destinations Event Filters Settings

+ Add Search Download Show/Hide Filter

Name	Notification Type	Destination	Associated Event Filters	Syslog Port	Syslog Transport
EMS-syslog	syslog	control.nva.local	smbc-aicum-nva-local_filter	514	tcp_unencrypted
smbc-aicum-nva-local_server	rest_api	https://smbc-aicum.nva.loc...	smbc-aicum-nva-local_filter	-	-
snmp-trapghost	snmp	-	default-trap-events	-	-

You can also configure ONTAP to send important Event Management System (EMS) event notifications by using the CLI. For example, the following command creates an event notification destination to send notifications to a syslog server. To resolve the syslog server name, DNS server must be configured on the cluster.

```
SiteA::> event notification destination create -name syslog-ems -syslog control.nva.local
```

You can create an event filter by using the `event filter create` command to build a filter that meets your specific event criteria. You can use the already defined event filters. You can check the event filters defined on the cluster by using the `event filter show` command.

```
SiteA:> event filter show
Filter Rule Rule
Name Posn Type Message Name Severity SNMP Trap
Type Parameters
-----
default-trap-events
      1 include * EMERGENCY, ALERT
      2 include callhome.* ERROR *
      3 include * Standard, Built-in
      4 exclude * * *
important-events
      1 include * EMERGENCY, ALERT
      2 include callhome.* ERROR *
      3 exclude * *
no-info-debug-events
      1 include * EMERGENCY, ALERT, ERROR, NOTICE
      2 exclude * *
...
```

The following example shows how you can create event notification with the `event notification create` command to forward `important-events` to the syslog server and check the event notification configuration with the `event notification show` command.

```
SiteA:> event notification create -filter-name important-events -destinations syslog-ems

SiteA:> event notification show
ID Filter Name Destinations
-----
1 default-trap-events snmp-traphost
2 smbc-aicum-nva-local_filter smbc-aicum-nva-local_server
3 important-events syslog-ems
3 entries were displayed.
```

VMware vSphere remote logging

Configure ESXi remote logging

You can configure the behavior of ESXi syslog files and transmissions by using a set of syslog options, including specifying a log host for remote logging.

To configure ESXi hosts for remote logging, log in to the ESXi hosts and use the `esxcli system syslog config set` command with the appropriate option parameters to configure remote logging. For example, the following command configures the remote syslog host, protocol, and port.

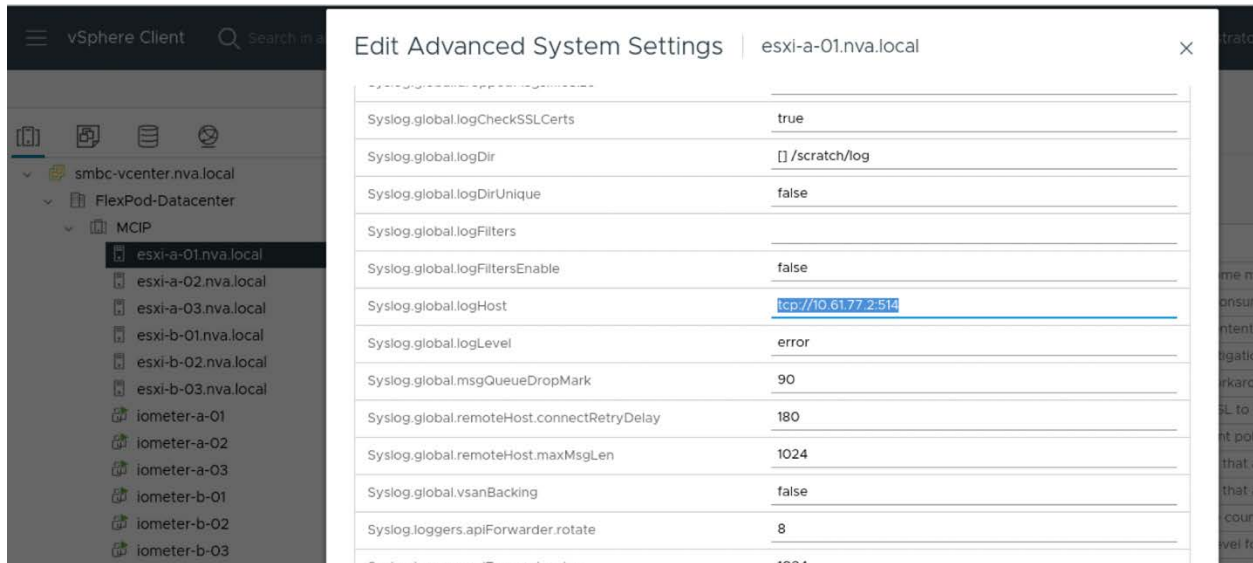
```
[root@esxi-a-01:~] esxcli system syslog config set --loghost=tcp://10.61.77.2:514
```

The `esxcli system syslog config get` command can be used to check the syslog configurations.

```
[root@esxi-a-01:~] esxcli system syslog config get
Allow Vsan Backing: false
Check Certificate Revocation List: false
Dropped Log File Rotation Size: 100
Dropped Log File Rotations: 10
Enforce SSLCertificates: true
Local Log Output: /scratch/log
Local Log Output Is Configured: false
Local Log Output Is Persistent: true
Local Logging Default Rotation Size: 1024
Local Logging Default Rotations: 8
```

```
Log Level: error
Log To Unique Subdirectory: false
Message Queue Drop Mark: 90
Remote Host: tcp://10.61.77.2:514
Remote Host Connect Retry Delay: 180
Remote Host Maximum Message Length: 1024
Strict X509Compliance: false
```

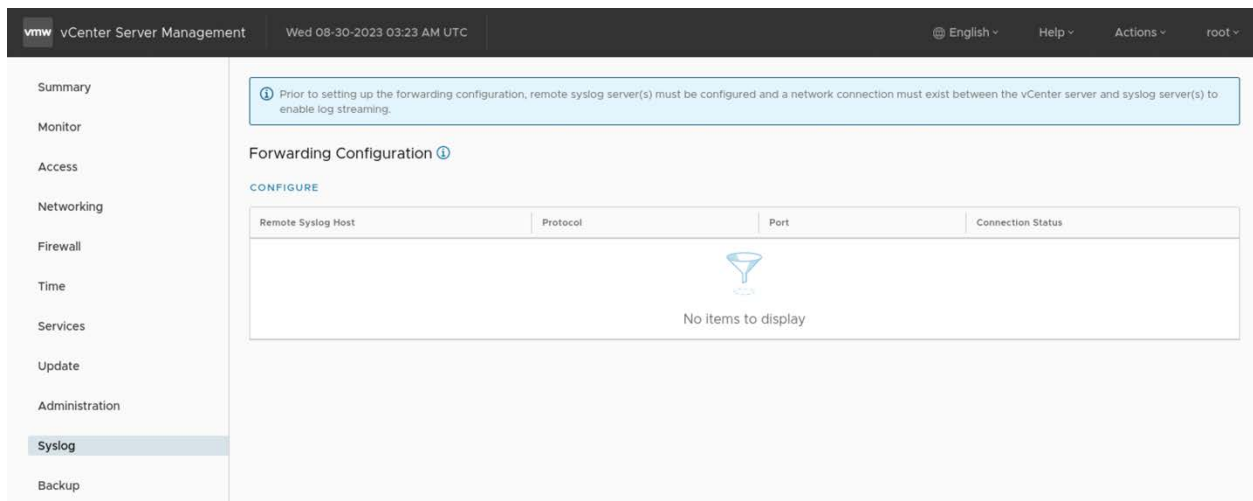
Note: You can also log in to vCenter Server, select the ESXi host, and edit Advanced System Settings that are related to the syslog configurations as shown in the screenshot below.



Forward vCenter Server log files to a remote syslog server

To forward the vCenter Server log files to a remote syslog server, log in to the vCenter Server Management Interface as root, and use the following steps to configure it.

Select Syslog in the vCenter Server Management Interface menu, then click Configure in the Forwarding Configuration section.



In the Create Forwarding Configuration pane, enter the remote syslog server address, protocol, and port information, and then click Save.

Create Forwarding Configuration

Specify forwarding configuration for remote syslog servers (no more than three).

Server Address	Protocol	Port
control.nva.local	TCP	514

[+ADD](#)

[CANCEL](#) [SAVE](#)

Click Send Test Message in the Forwarding Configuration section and then click Send in the Send Test Message dialog to send a test message to the syslog server.

Forwarding Configuration ⓘ

[EDIT](#) [SEND TEST MESSAGE](#) [DELETE](#)

Remote Syslog Host	Protocol	Port	Connection Status
control.nva.local	TCP	514	Reachable

Send Test Message

Manually verify from remote syslog servers if the message has been received.

Test message: This is a diagnostic syslog test message from vCenter Server.

Servers: control.nva.local

[CANCEL](#) [SEND](#)

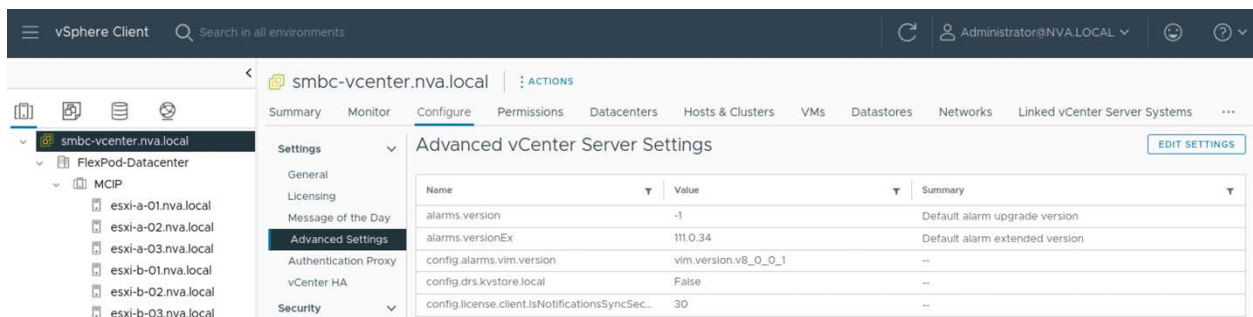
Check on the syslog server to confirm that the diagnostic test message from vCenter Server was received.

```
$ sudo cat /var/log/messages | grep "diagnostic syslog"
Aug 30 20:13:13 smbc-vcenter - This is a diagnostic syslog test message from vCenter Server.
```

Streaming vCenter Server events to a remote syslog server

You can enable and configure vCenter Server to stream events to a remote syslog server from the Center Server Management Interface.

Login to vCenter Server, select Configure tab, expand Settings option, select Advanced Settings, click Edit Settings.



Click on the filter icon in the Name column, type in vpxd.event in the filter pop-up box, and then close the filter box. Check to make sure that the vpxd.event.syslog.enabled option in the filtered down option list is showing enabled, and then click Save.

Edit Advanced vCenter Server Settings

ⓘ Adding or modifying configuration parameters is unsupported and can cause instability. Configuration parameters cannot be removed once they are added. Continue only if you know what you are doing.

Name	Value	Summary
vpxd.event.burstFilter.compressToDb	<input checked="" type="checkbox"/> Enabled	Enable compression of bursting events to the database
vpxd.event.burstFilter.compressToSyslog	<input type="checkbox"/> Enabled	Enable compression of bursting events to the syslog stream
vpxd.event.syslog.enabled	<input checked="" type="checkbox"/> Enabled	Enable streaming of events to syslog

1 - 5 of 5 settings

Name *: _____ Value: _____ ADD

Name must start with 'config.' For example: config.log

CANCEL SAVE

Note: Be sure to check the space consumption of the log files on the syslog server and adjust logging level and/or log retention / rotation policies so you can keep sufficient logs while not running out of space.

Configuration backup

It is a best practice to setup scheduled backup of FlexPod component configurations. A backup server must be already set up and configured such that the FlexPod components have access to it using a protocol supported by their configuration backup.

Cisco UCS Manager configuration backup

The configuration of the Cisco UCS Manager can be backed up manually at any time and automated backups can also be enabled. To enable the automatic configuration backup, use the following steps.

Log in to Cisco UCS Manager and select Admin > All > Policy Backup & Export. Under All Configuration Backup Policy, configure the various information appropriate for your configuration backup. Please note that you will need to Enable the Admin State before you can fill in the Remote File field.

The screenshot displays the Cisco UCS Manager interface. On the left is a navigation sidebar with a tree view. The 'All' menu item is selected, and the 'Policy Backup & Export' sub-item is highlighted. The main content area is titled 'All' and contains two tabs: 'General' and 'Policy Backup & Export'. The 'Policy Backup & Export' tab is active, showing configuration for two backup policies.

Full State Backup Policy

- Hostname :
- Protocol : ☐ FTP ☐ TFTP ☒ SCP ☐ SFTP
- User :
- Password :
- Remote File :
- Admin State : ☒ Disable ☐ Enable
- Schedule : ☐ Daily ☒ Weekly ☐ Bi Weekly
- Max Files : **0**
- Description :

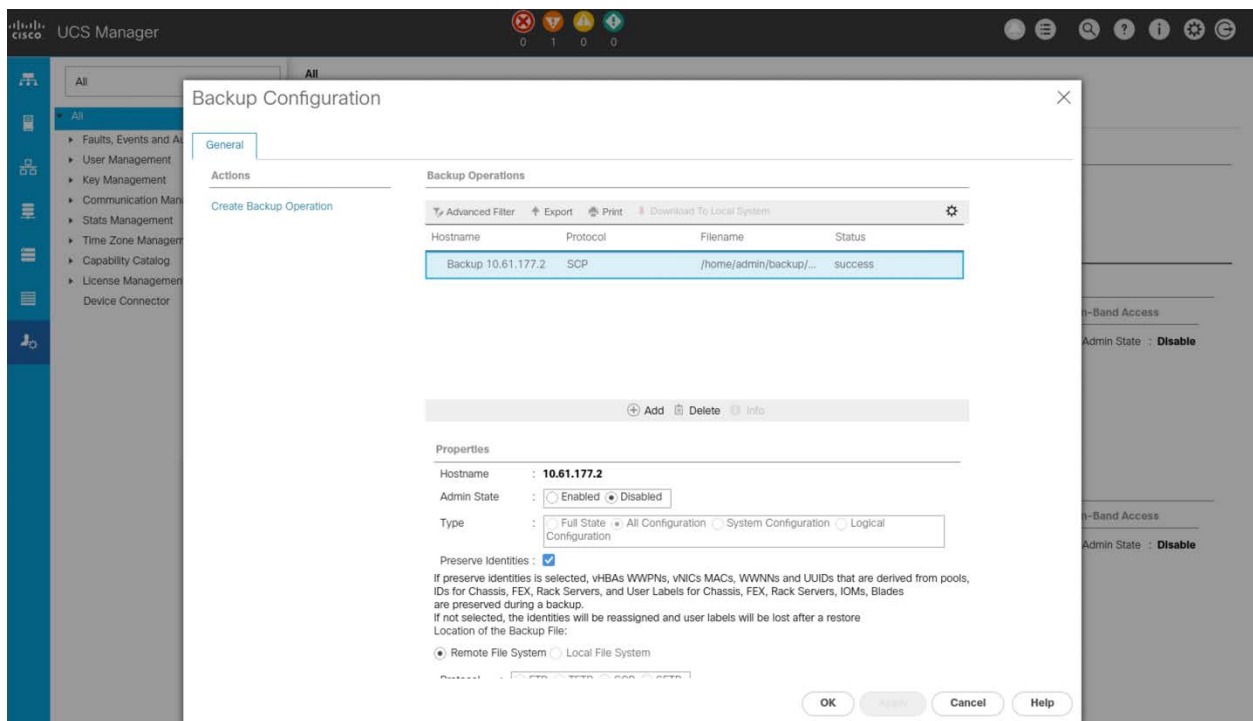
All Configuration Backup Policy

- Hostname :
- Protocol : ☐ FTP ☐ TFTP ☒ SCP ☐ SFTP
- User :
- Password :
- Remote File :
- Admin State : ☐ Disable ☒ Enable
- Schedule : ☒ Daily ☐ Weekly ☐ Bi Weekly
- Max Files : **0**
- Description :

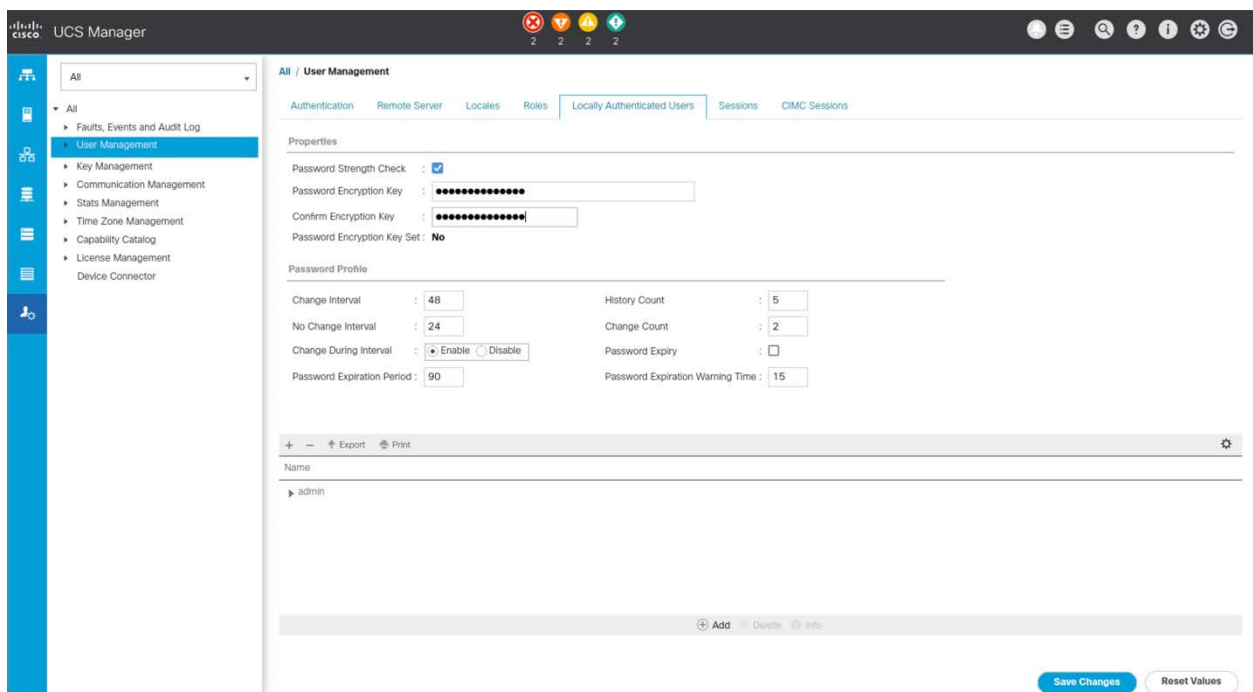
Backup/Export Config Reminder

- Admin State : ☐ Disable ☒ Enable

Click the General tab and select Backup Configuration. After a few minutes, you can see the scheduled backup in this window.



Note: For these backups to complete correctly, the Password Encryption Key must be set under Admin > All > User Management > Locally Authenticated Users.



Cisco Nexus configuration backup

The configurations of the Cisco Nexus 9000 switches can be backed up manually at any time with the copy command and automated scheduled backups can be enabled by using the NX-OS scheduler feature.

For the scheduled configuration backup to use scp protocol without specifying password each time, we need to create SSH keys for the user and transfer the public key into the SSH server where the configuration backup will be copied over.

The following shows an example of generating a pair of ssh public key and private key in the global configuration mode for the admin user and showing the generated public key information.

```
SiteA-switch-a.nva.local# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SiteA-switch-a.nva.local(config)# username admin keypair generate rsa 2048 force

SiteA-switch-a.nva.local(config)# show username admin keypair
*****

rsa Keys generated:Fri Oct 27 20:26:20 2023

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQCuRpcqJpMS4Wrhtt+F4w2dJBuNn6u0iQsNCpxeY0u5Qx8BoE9kuByofkWNd9a9mlrIS
HNPEbdZChznH
tI12R+RmOuwFN+crJloiM/93CZhcW7ugDuBzqqhJNWBRIEjayTsXbtG5vhPLIGFi j61B1XXsMgz4j3ciWhkwVxnKSicMrjS8n
0qLosAewwNY9v1Y09YQQ
lApuhnhMVpMpl/Za4y6C46msgZuTDV3s+M2VRVAv1AKCWsC85xCrgw01Kh0Ih4k7JIBxlC+lew14ZLSbnLKdbQ2u77u1NKiHY
C2p5TwrmsYK5r8CZ/eKp
Go9jBTXY8z3OfK2spGBSDeghHSSsJ

bitcount:2048
fingerprint:
SHA256:3HT4hqqQxpUEH2/23xSxZ2+byUTFrH/0Vz/GdxqU40o*****

could not retrieve dsa key information
*****

could not retrieve ecdsa key information
*****
SiteA-switch-a.nva.local(config)#
```

To transfer the generated public key into the SSH server, we need to export the previously generated keys. The export command shown in the example below requested for a passphrase to be entered and then created the key_rsa and key_rsa.pub files in the bootflash.

```
SiteA-switch-a.nva.local(config)# username admin keypair export bootflash:key_rsa rsa force
Enter Passphrase:
SiteA-switch-a.nva.local(config)#
```

The following shows an example of copying the public key file in the bootflash over to the SSH server.

```
SiteA-switch-a.nva.local(config)# copy bootflash:key_rsa.pub
scp://admin@10.61.177.2/home/admin/key_rsa.pub
Enter vrf (If no input, current vrf 'default' is considered): management
Inbound-ReKey for 10.61.177.2:22
admin@10.61.177.2's password:
key_rsa.pub                                                    100%  411
207.3KB/s   00:00
Copy complete, now saving to disk (please wait)...
Copy complete.
SiteA-switch-a.nva.local(config)#
```

On the backup server, append the public key stored in the key_rsa.pub file to the authorized_keys file.

```
[admin@control ~]$ cat key_rsa.pub >> $HOME/.ssh/authorized_keys

[admin@control ~]$ chmod 0700 $HOME/.ssh
[admin@control ~]$ chmod 0600 $HOME/.ssh/authorized_keys
```

Note: If this is the first time a key is being added to the authorized_keys file, the newly created authorized_keys file may not have the right permission for the SSH server to consume. The

chmod commands above updated the directory and file permissions for them to be compliant.

After the public key is in place, we can manually backup the switch configuration using scp without needing to specify the password.

```
SiteA-switch-a.nva.local# copy running-config
scp://admin@10.61.177.2/home/admin/backup/Nexus/SiteA-switch-a.cfg vrf management
Inbound-ReKey for 10.61.177.2:22
SiteA-switch-a.nva.local-running-config                                100%   19KB
4.9MB/s   00:00
Copy complete, now saving to disk (please wait)...
Copy complete.
```

Note: The directory /home/admin/backup/Nexus had already been created previously.

The following is an example of configuration backup scheduling for one of the Nexus switches.

```
SiteA-switch-a.nva.local# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
SiteA-switch-a.nva.local(config)# feature scheduler
SiteA-switch-a.nva.local(config)# scheduler logfile size 1024
SiteA-switch-a.nva.local(config)# scheduler job name backup-cfg
SiteA-switch-a.nva.local(config-job)# copy running-config
scp://admin@10.61.177.2/home/admin/backup/Nexus/${SWITCHNAME}-cfg.${TIMESTAMP} vrf management
SiteA-switch-a.nva.local(config-job)# exit
SiteA-switch-a.nva.local(config)# scheduler schedule name daily
SiteA-switch-a.nva.local(config-schedule)# job name backup-cfg
SiteA-switch-a.nva.local(config-schedule)# time daily 2:00
SiteA-switch-a.nva.local(config-schedule)# end
```

Note: Using “vrf management” in the copy command is only needed when Mgmt0 interface is part of VRF management.

The show schedule job and show scheduler schedule commands can be used to verify that the backup job and schedule have been correctly set up. Save the configuration changes by copying the running-config to startup-config.

```
SiteA-switch-a.nva.local# show scheduler job
Job Name: backup-cfg
-----
copy running-config scp://admin@10.61.177.2/backup/Nexus/${SWITCHNAME}-cfg.${TIMESTAMP} vrf
management

=====

SiteA-switch-a.nva.local# show scheduler schedule
Schedule Name      : daily
-----
User Name          : admin
Schedule Type      : Run every day at 2 Hrs 0 Mins
Last Execution Time : Yet to be executed
-----
Job Name           Last Execution Status
-----
backup-cfg         -NA-
=====

SiteA-switch-a.nva.local# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
```

After the scheduled backup time, you can check the backup server for the existence of the switch configuration backup files.

```
[admin@control ~]$ ls -l /home/admin/backup/Nexus
total 80
```

```
-rw-rw-r--. 1 admin admin 19909 Oct 29 22:00 SiteA-switch-a.nva.local-cfg.2023-10-30-02.00.01
-rw-rw-r--. 1 admin admin 18228 Oct 29 22:00 SiteA-switch-b.nva.local-cfg.2023-10-30-02.00.01
-rw-rw-r--. 1 admin admin 17608 Oct 29 22:00 SiteB-switch-a.nva.local-cfg.2023-10-30-02.00.00
-rw-rw-r--. 1 admin admin 17068 Oct 29 22:00 SiteB-switch-b.nva.local-cfg.2023-10-30-02.00.01
```

NetApp ONTAP configuration backup

The configuration backup files of the NetApp ONTAP cluster and nodes are automatically created according to the following schedules:

- Every 8 hours
- Daily
- Weekly

At each of these times, a node configuration backup file is created on each healthy node in the cluster. All these node configuration backup files are then collected in a single cluster configuration backup file along with the replicated cluster configuration and saved on one or more nodes in the cluster.

An example of viewing the ONTAP cluster configuration backup files in advanced privilege mode is shown below:

```
SiteA::> set advanced

Warning: These advanced commands are potentially dangerous; use them only when directed to do so
by NetApp personnel.
Do you want to continue? {y|n}: y

SiteA::> system configuration backup show
Node      Backup Name                                     Time                               Size
-----
SiteA-03  SiteA.8hour.2023-09-04.18_15_00.7z             09/04 18:15:00                     67.79MB
SiteA-03  SiteA.8hour.2023-09-05.02_15_03.7z             09/05 02:15:03                     70.10MB
SiteA-03  SiteA.8hour.2023-09-05.10_15_03.7z             09/05 10:15:03                     70.46MB
SiteA-03  SiteA.daily.2023-09-04.00_10_00.7z             09/04 00:10:00                     70.43MB
SiteA-03  SiteA.daily.2023-09-05.00_10_00.7z             09/05 00:10:00                     69.36MB
SiteA-03  SiteA.weekly.2023-08-27.00_15_00.7z            08/27 00:15:00                     68.50MB
SiteA-03  SiteA.weekly.2023-09-03.00_15_00.7z            09/03 00:15:00                     69.32MB
SiteA-04  SiteA.8hour.2023-09-05.02_15_03.7z             09/05 02:15:03                     70.10MB
SiteA-04  SiteA.8hour.2023-09-05.10_15_03.7z             09/05 10:15:03                     70.46MB
SiteA-04  SiteA.daily.2023-09-03.00_10_00.7z             09/03 00:10:00                     69.21MB
SiteA-04  SiteA.daily.2023-09-04.00_10_00.7z             09/04 00:10:00                     70.43MB
SiteA-04  SiteA.daily.2023-09-05.00_10_00.7z             09/05 00:10:00                     69.36MB
SiteA-04  SiteA.weekly.2023-08-20.00_15_03.7z            08/20 00:15:03                     37.59MB
SiteA-04  SiteA.weekly.2023-08-27.00_15_00.7z            08/27 00:15:00                     68.50MB
SiteA-04  SiteA.weekly.2023-09-03.00_15_00.7z            09/03 00:15:00                     69.32MB
15 entries were displayed.

SiteA::> set admin
SiteA::>
```

You can use system configuration backup settings commands in advanced mode to manage configuration backup schedules and specify a remote URL (HTTP, HTTPS, FTP, FTPS, or TFTP) where the configuration backup files will be uploaded in addition to the default locations in the cluster.

An example of setting up an automated ONTAP cluster configuration backup upload destination, username, and password is shown below:

```
SiteA::> set advanced

Warning: These advanced commands are potentially dangerous; use them only when directed to do so
by NetApp personnel.
Do you want to continue? {y|n}: y

SiteA::> system configuration backup settings modify -destination
ftp://control.nva.local/home/admin/backup/ONTAP -username admin
```

```

SiteA::*> system configuration backup settings show
Backup Destination URL                               Username
-----
ftp://control.nva.local/home/admin/backup/ONTAP      admin

SiteA::*> system configuration backup settings set-password

Enter the password:
Confirm the password:

SiteA::*> set admin
SiteA::>



```

VMware vCenter Sever backup

A backup server must be already set up and configured such that the vCenter Server has access to it using HTTP, HTTPS, SFTP, FTP, FTPS, NFS, or SMB protocols. To schedule automatic backup of the vCenter Server Appliance, log into to the vCenter Server Management Interface as the root user and perform the following steps.

Select Backup from the left menu and click Configure to the right of Backup Schedule. In the Create Backup Schedule pop-up window, specify the backup location with the transfer protocol, the username and password for the backup server, the backup schedule, the number of backups to retain, and the type of data to backup.

Create Backup Schedule

Backup location *			ftp://control.nva.local/home/admin/backup/VCSA
Backup server credentials	User name	admin	
	Password	••••••••••	
Schedule 	Daily ▾	02 : 15	A.M. US/Eastern
Encrypt backup	Encryption Password		
	Confirm Password		
Number of backups to retain *	<input type="radio"/> Retain all backups		
	<input checked="" type="radio"/> Retain last <input type="text" value="7"/> backups		
Data	<input checked="" type="checkbox"/> Stats, Events, and Tasks	88 MB	
	<input checked="" type="checkbox"/> Inventory and configuration	1057 MB	
	Total size (compressed)		1145 MB
		<input type="button" value="CANCEL"/>	<input type="button" value="CREATE"/>

Click Create to create the specified backup schedule. Expand Status under the Backup Schedule to confirm the schedule information.

Backup Schedule		EDIT	DEACTIVATE	DELETE
▼ Status	Activated			
Schedule	Daily , 2:15 A.M. US/Eastern			
Backup Location	ftp://control.nva.local/home/admin/backup/VCSA			
Backup data	<ul style="list-style-type: none"> • Stats, Events, and Tasks • Inventory and configuration 			
Number of backups to retain	7			

FIPS 140 compliance

The Federal Information Processing Standard 140 (FIPS 140) is a U.S. government standard that sets security requirements for cryptographic modules in hardware, software, and firmware to protect sensitive information. Compliance with the standard is mandated for use by U.S. government agencies, and it is also often used in industries such as financial services and healthcare.

Under the FIPS 140 standard, both the algorithm and the module are evaluated for compliance, using programs that are jointly developed by the U.S. National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS).

The Cryptographic Module Validation Program (CMVP) is the accreditation program for cryptographic module security. The Cryptographic Algorithm Validation Program (CAVP) provides guidelines for validating the effectiveness of FIPS-approved and NIST-recommended cryptographic algorithms.

FIPS 140 security requirements encompass 11 areas related to the design, strength, and operation of a cryptographic module. In each of the 11 areas, there are four security levels. Level 1 is the least restrictive, specifying the lowest level of security, and Level 4 specifies the highest level.

Note: Please see links in the reference section for more FIPS compliance information available from NetApp, Cisco, and VMware.

Cisco UCS FIPS 140 compliance

By default, Cisco UCS Manager works in the Federal Information Processing Standards (FIPS) mode. In the FIPS mode, the DSA key is not supported.

However, the Cisco UCS C-Series Server Integrated Management Controller (CIMC) does not have FIPS mode enabled by default. Please refer to the documentation listed in the reference to enable FIPS mode for the UCS C-Series servers.

Cisco Nexus FIPS 140 compliance

Enable FIPS mode

Cisco NX-OS devices support FIPS mode. It has the following prerequisites, configuration guidelines, and limitations.

- Disable Telnet. Users should log in using Secure Shell (SSH) only.
- Disable SNMPv1 and v2. Any existing user accounts on the device that have been configured for SNMPv3 should be configured only with SHA for authentication and AES/3DES for privacy.
- Delete all SSH server RSA1 key-pairs.
- Enable HMAC-SHA1 message integrity checking (MIC) for use during the Cisco TrustSec Security Association Protocol (SAP) negotiation. To do so, enter the `sap hash-algorithm HMAC-SHA-1` command from the `cts-manual` or `cts-dot1x` mode.
- The user authentication mechanisms supported for SSH are usernames and passwords, public keys, and X.509 certificates.

- Your passwords should have a minimum of eight alphanumeric characters.
- Disable Radius and TACACS when FIPS mode is on. This is enforced due to OpenSSL in FIPS mode.

By default, FIPS mode is disabled on the Cisco NX-OS devices. To enable FIPS mode on the Cisco NX-OS devices, perform the following steps on all FlexPod switches.

Re-generate RSA key with 2048 key bits from the console, if the switch was initialized with an RSA key which was not using 2048 key bits. In the example output below, the actual key information has been removed as noted.

```
SiteA-switch-a.nva.local# conf terminal
Enter configuration commands, one per line. End with CNTL/Z.

SiteA-switch-a.nva.local(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled

SiteA-switch-a.nva.local(config)# no ssh key rsa

SiteA-switch-a.nva.local(config)# ssh key rsa 2048

SiteA-switch-a.nva.local(config)# show ssh key
*****
rsa Keys generated:Sun Aug 27 02:45:42 2023

ssh-rsa [removed]

bitcount:2048
fingerprint:
SHA256:[removed]
*****
could not retrieve dsa key information
*****
could not retrieve ecdsa key information
*****

SiteA-switch-a.nva.local(config)# feature ssh

SiteA-switch-a.nva.local(config)# exit

SiteA-switch-a.nva.local# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
```

Enter global configuration mode to enable FIPS mode. After FIPS mode is enabled, reboot the switch for the FIPS mode to take effect as instructed.

```
SiteA-switch-a.nva.local# conf terminal
Enter configuration commands, one per line. End with CNTL/Z.

SiteA-switch-a.nva.local(config)# fips mode enable
FIPS mode is enabled
System reboot is required after saving the configuration for the system to be in FIPS mode

2023 Aug 27 03:03:09 SiteA-switch-a.nva.local %$ VDC-1 %$ %USER-2-SYSTEM_MSG: FIPS mode is
Enabled for service securityd - securityd

SiteA-switch-a.nva.local(config)# exit

SiteA-switch-a.nva.local# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.

SiteA-switch-a.nva.local# reload
This command will reboot the system. (y/n)? [n] y
```

Check FIPS status after the switch is rebooted.

```
SiteA-switch-a.nva.local# show fips status
FIPS Status: enabled
Switch Mode: FIPS
-----
LC          STATUS
-----
```

NetApp ONTAP FIPS 140 compliance

Enable FIPS mode

NetApp ONTAP data management software has a FIPS mode configuration that instantiates an added level of security for the customer. This FIPS mode applies to the control plan and secures all control Interfaces of ONTAP.

When FIPS mode is enabled, there are related security practices that will be enforced.

- Transport Layer Security v1.1 (TLSv1.1) is disabled, and only TLS v1.2 and TLS v1.3 remain enabled.
- An SNMP users or SNMP traphosts that are non-compliant to FIPS will be deleted automatically.
- An SNMPv1 user, SNMPv2c user or SNMPv3 user (with none or MD5 as authentication protocol or none or DES as encryption protocol or both) is non-compliant to FIPS.
- An SNMPv1 traphost or SNMPv3 traphost (configured with an SNMPv3 user non-compliant to FIPS) is non-compliant to FIPS.

In addition, before you enable FIPS mode on your cluster, existing SSH public key accounts without the supported key algorithms must be reconfigured with a supported key type. The accounts should be reconfigured before you enable FIPS or the administrator authentication will fail. Table 11 lists host key type algorithms that are supported for ONTAP SSH connections.

Table 11) Supported host key type algorithms for ONTAP SSH connections

ONTAP release	Key types supported in FIPS mode	Key types supported in non-FIPS mode
9.11.1 and later	ecdsa-sha2-nistp256	ecdsa-sha2-nistp256 rsa-sha2-512 rsa-sha2-256 ssh-ed25519 ssh-dss ssh-rsa
9.10.1 and earlier	ecdsa-sha2-nistp256 ssh-ed25519	ecdsa-sha2-nistp256 ssh-ed25519 ssh-dss ssh-rsa

By default, the FIPS 140-2 mode is disabled on the ONTAP cluster. To enable FIPS mode on the ONTAP cluster, elevate privilege from admin to advanced mode and use the `security config modify` command to enable it.

```
SiteA::> set advanced
Warning: These advanced commands are potentially dangerous; use them only when directed to do so
by NetApp personnel.
Do you want to continue? {y|n}: y

SiteA::> security config modify * -is-fips-enabled true

Warning: This command will enable FIPS compliance and can potentially cause some non-compliant
components to fail. MetroCluster and Vserver DR require FIPS to be enabled on both sites in order
```

```

to be compatible. An SNMP users or SNMP traphosts that are non-compliant to FIPS will be deleted
automatically. An SNMPv1 user, SNMPv2c user or SNMPv3 user (with none or MD5 as authentication
protocol or none or DES as encryption protocol or both) is non-compliant to FIPS. An SNMPv1
traphost or SNMPv3 traphost (configured with an SNMPv3 user non-compliant to FIPS) is non-
compliant to FIPS.
Do you want to continue? {y|n}: y
1 entry was modified.

```

The protocols and cipher suites supported by ONTAP can be retrieved by using the `security config show` command. The following provides a truncated output from that command. Please note that the supported protocols and cipher suites for ONTAP can be further restricted by using the `security config modify` command and providing a list of protocols and cipher suites with `-supported-protocols` and `-supported-cipher-suites` options.

```

SiteA::*> security config show
Cluster      Supported
FIPS Mode    Protocols Supported Cipher Suites
-----
true         TLSv1.3,    TLS_RSA_WITH_AES_128_CCM, TLS_RSA_WITH_AES_128_CCM_8,
            TLSv1.2     TLS_RSA_WITH_AES_128_GCM_SHA256,
            TLS_RSA_WITH_AES_128_CBC_SHA,
            TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CCM,
            TLS_RSA_WITH_AES_256_CCM_8,
            TLS_RSA_WITH_AES_256_GCM_SHA384,
            TLS_RSA_WITH_AES_256_CBC_SHA,
            TLS_RSA_WITH_AES_256_CBC_SHA256,
            TLS_DHE_DSS_WITH_AES_128_GCM_SHA256,
            TLS_DHE_DSS_WITH_AES_128_CBC_SHA,
            ...

```

VMware vSphere FIPS 140 compliance

To protect management interface and VMware Certificate Authority (VMCA), ESXi 8 and vCenter Server 8 use FIPS 140-2 validated cryptographic. For a list of FIPS modules supported by ESXi, please refer to the vSphere Security documentation listed in the reference.

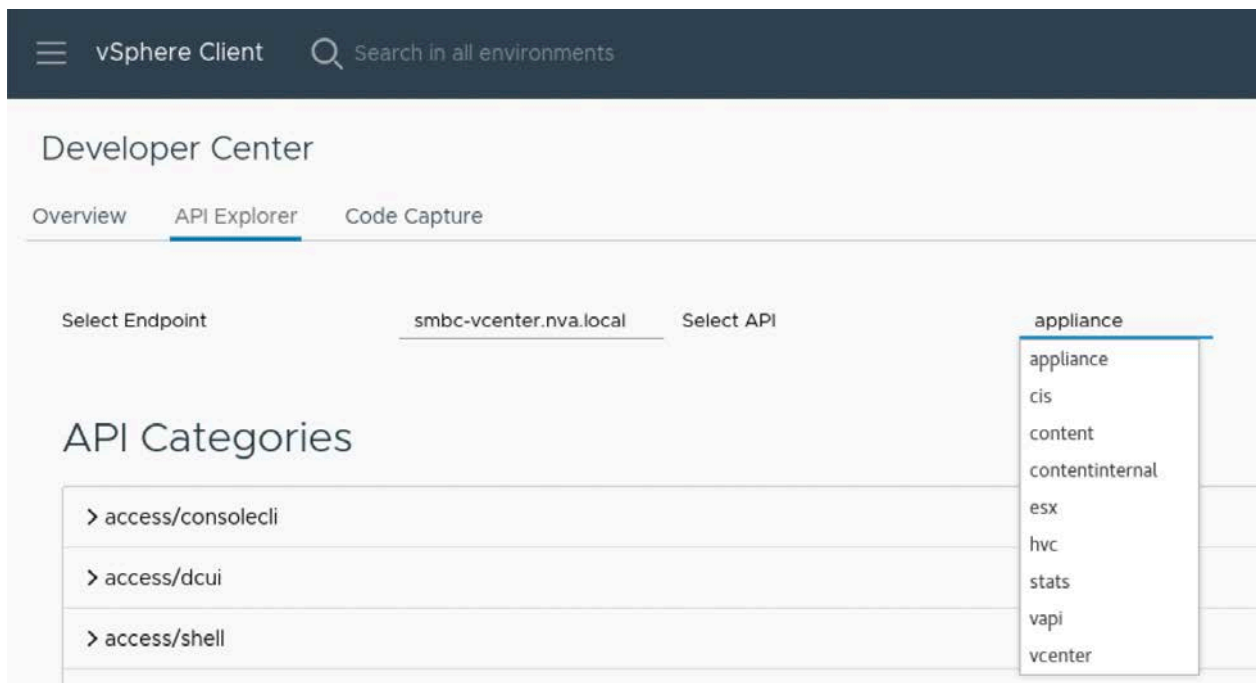
You can enable FIPS-validated cryptography for vCenter Server. However, before activating FIPS on vCenter Server, you need to be aware of the following considerations.

- vSphere Single Sign-on supports only cryptographic modules for federated authentication.
- vSphere Client UI plug-ins from partners which are not FIPS compliant might not work.
- Use 2048- or 3072-bit key sizes for certificates as key sizes greater than 3072 bits have not been tested.

Enable FIPS on vCenter Server

To activate FIPS for vCenter Server, log in to vCenter Server with vSphere Client and perform the following steps.

Select Developer Center from the Menu, click on API Explorer tab, and select appliance from the Select API dropdown list.



Search the API Categories for system and expand the system/security/global_fips category.



Expand Get and click Execute under Try it out.

system/security/global_fips

GET

/api/appliance/system/global-fips

Response types

Code/Reason	Model
200 Current FIPS settings state.	ApplianceSystemSecurityGlobalFipsInfo { ... }
500 Generic error	VapiStdErrorsError { ... }

Try it out

EXECUTE

✓

DOWNLOAD

View the current setting under Response.

Try it out

EXECUTE

✓

DOWNLOAD

Curl

curl -X GET 'https://smbc-vcenter.nva.local/api/appliance/system/global-fips' -H 'vmware-api-session-id: 13de0f0fd13c3e3df025ac0946cc882c'

Response

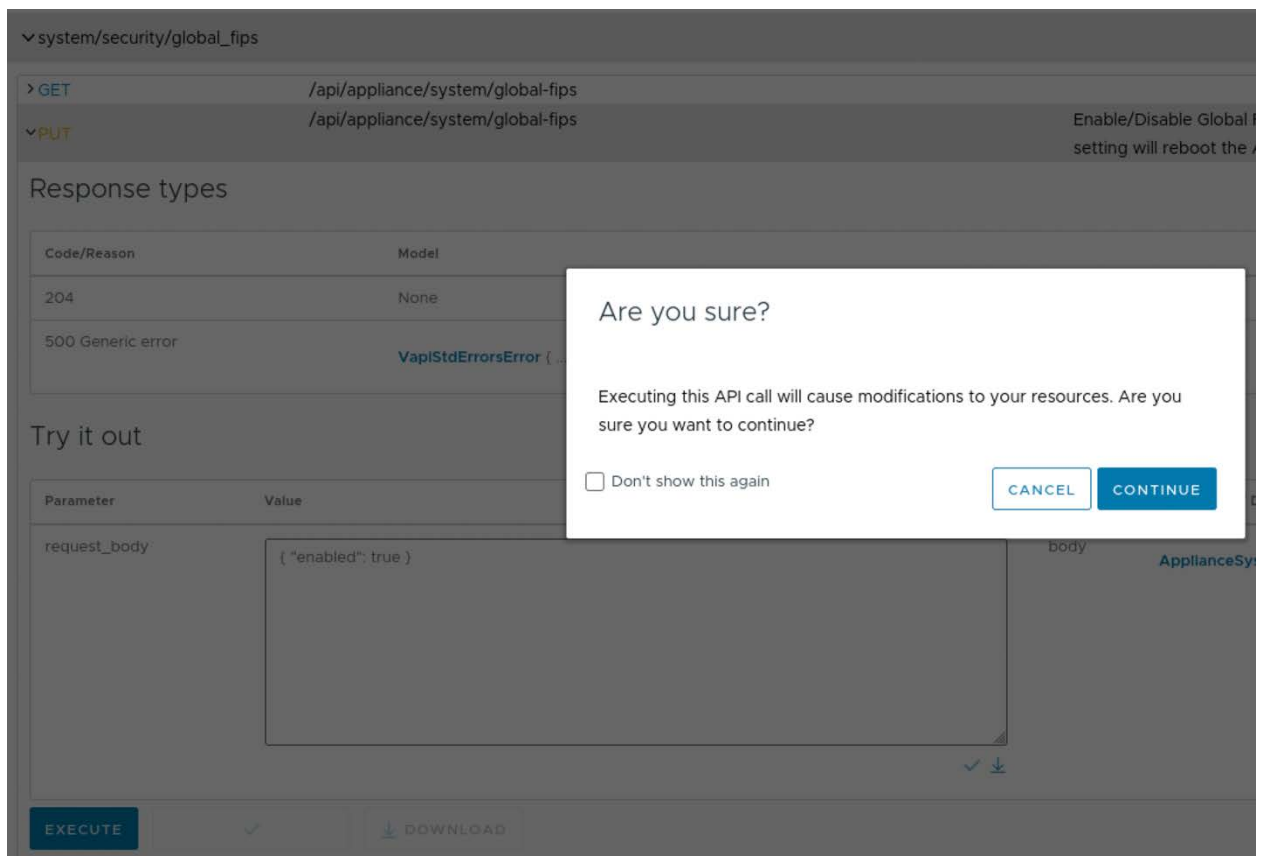
[ApplianceSystemSecurityGlobalFipsInfo](#) ✓ ⬇ {

enabled: (boolean, required) false,

}

To activate FIPS, expand Put and enter the following value for the request_body parameter, click Execute, and click Continue for the change confirmation.

{ "enabled": true }



After the confirmation, vCenter Server reboots for the change to take effect.

After vCenter Server is rebooted, go back to the system/security/global_fips API to execute Get and confirm that the response shows FIPS is now activated.

Developer Center

Overview API Explorer Code Capture

recovery/backup/system_name/archive

system/security/global_fips

GET /api/appliance/system/global-fips

Response types

Code/Reason	Model
200 Current FIPS settings state.	ApplianceSystemSecurityGlobalFipsInfo { ... }
500 Generic error	VapiStdErrorsError { ... }

Try it out

EXECUTE ☐

Curl

```
curl -X GET 'https://smbc-vcenter.nva.local/api/appliance/system/global-fips' -H 'vmware-api-session-id: 4b6806a2d2fde70ff29d465a331ec49'
```

Response

```
ApplianceSystemSecurityGlobalFipsInfo ✓ ⬇ {
  "enabled": "true", true,
}
```

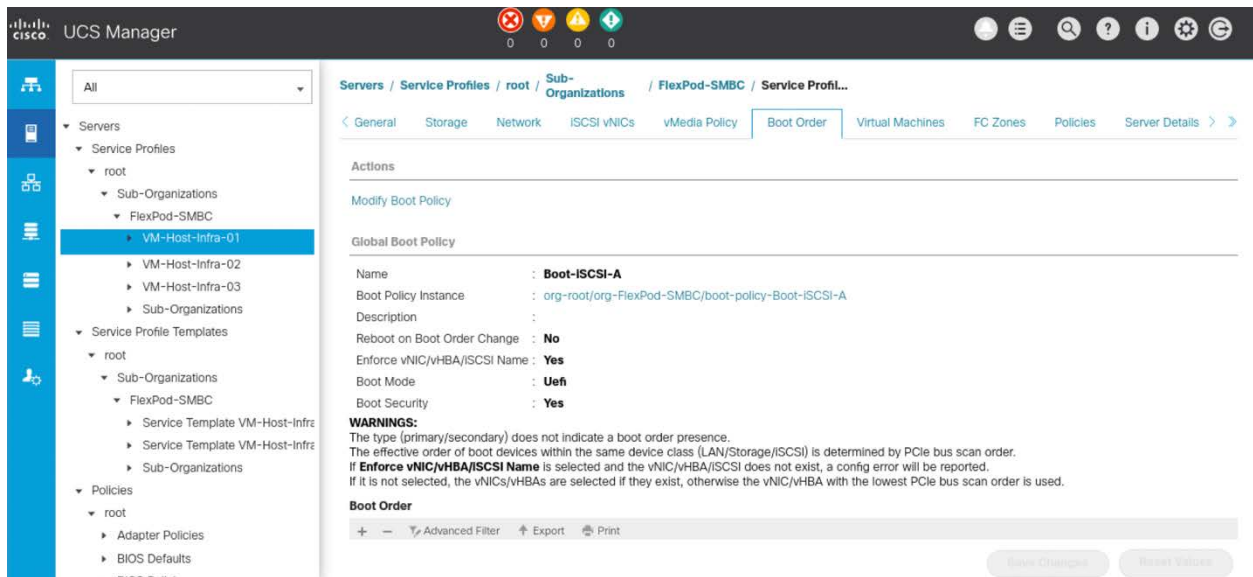
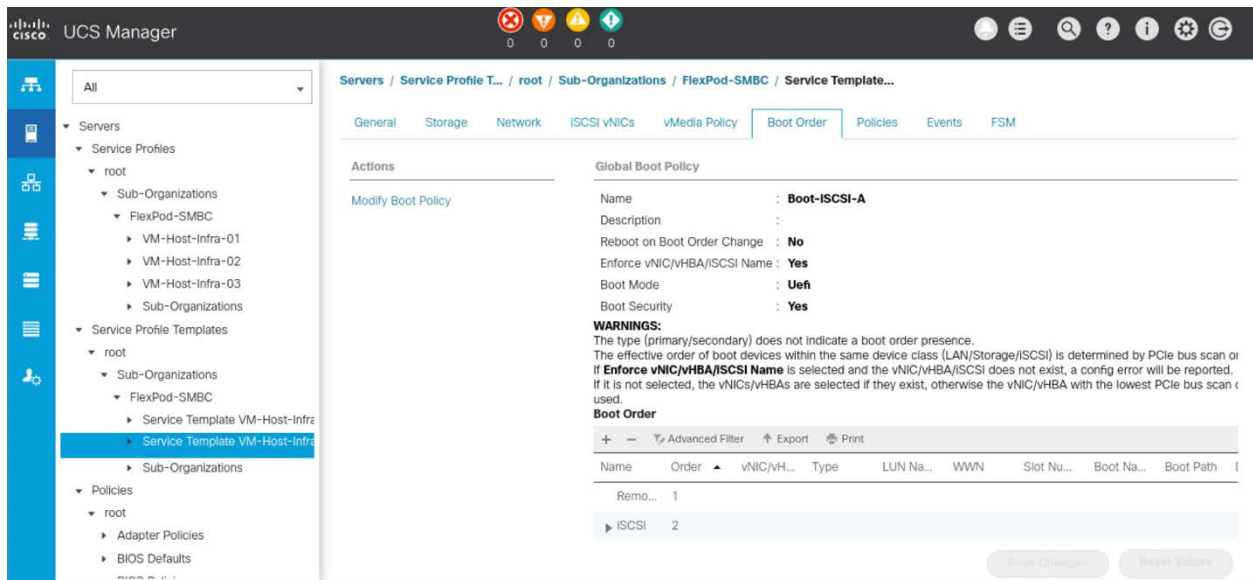
UEFI secure boot

Cisco UCS Manager supports Unified Extensible Firmware Interface (UEFI), which is a specification that defines a software interface between an operating system and platform firmware. In UCS Manager, UEFI can be used to replace the BIOS firmware interfaces. When BIOS is running in UEFI mode, it still provides legacy support. When UEFI secure boot is enabled, BIOS authenticates all executables, such as boot loaders and adapter drivers, before loading them.

The Trusted Platform Module (TPM) is a component that can be used to authenticate the server by using its securely store artifacts such as passwords, certificates, and encryption keys. A TPM can also be used to help ensure that the platform remains trustworthy.

Cisco UCS Manager secure boot

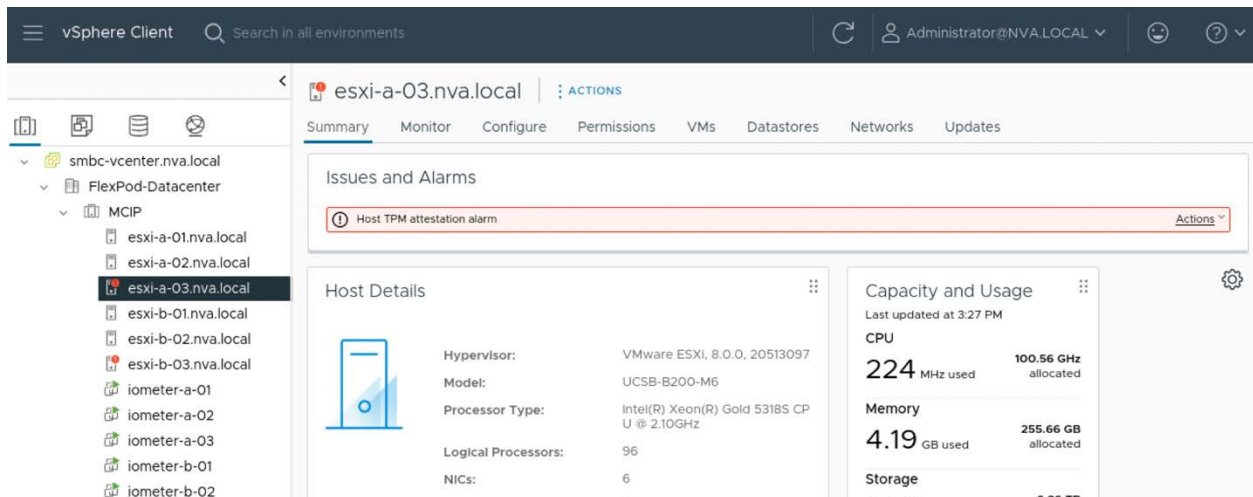
In a FlexPod configuration, UEFI secure boot is enabled in the Cisco UCS boot order policy configuration. To check a service profile template, or a service profile, for UEFI secure boot configuration, click on the service profile template, or service profile, and examine the Boot Mode and Boot Security settings in the Boot Order tab to confirm that Boot Mode is Uefi and Boot Security is Yes. See screenshots below for examples.



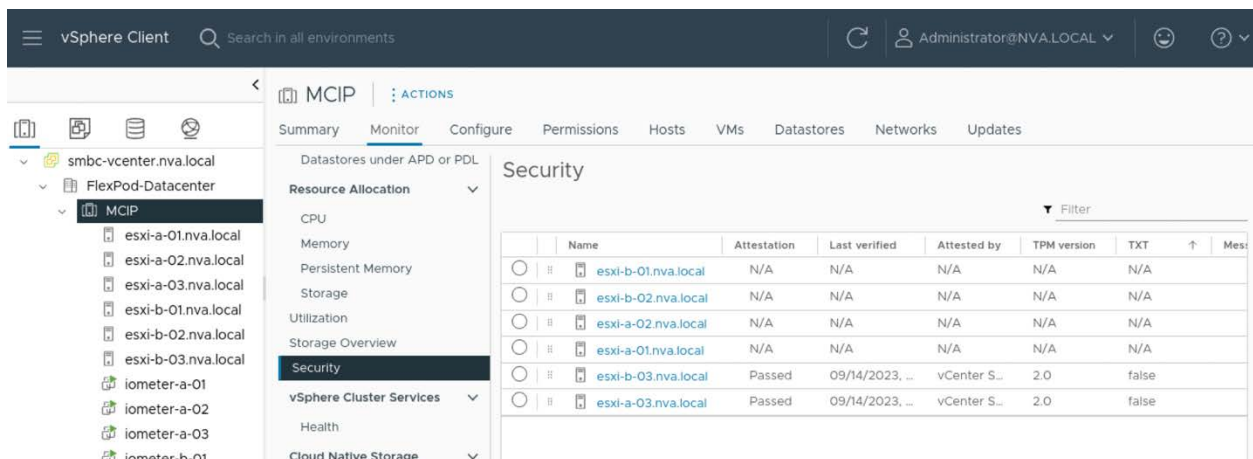
VMware vCenter Server secure boot attestation

If your Cisco UCS server have a TPM 2.0 module installed, the TPM module can provide assurance that ESXi has booted with UEFI secure boot enabled and is using only digitally signed code. In addition, VMware vCenter server can attest that the server is booted with UEFI secure boot.

When you migrate an ESXi host from a server without a TPM 2.0 module to a server that has a TPM 2.0 module and UEFI secure boot is enabled in the service profile, vCenter Server will report a Host TPM attestation alarm. You can acknowledge the issue and resolve it by disconnecting the host from vCenter Server and then reconnecting it.



To confirm UEFI secure boot in vCenter Server, log in to vSphere Client, select cluster under Hosts and Clusters, click Monitor tab in the center pane, and select Security. vCenter Server shows the TPM attestation status as well as the TPM version for the hosts. In the example below, two of the ESXi hosts have the TPM 2.0 module installed and they both passed vCenter Server attestation.



VMware ESXi secure boot

You should enable secure boot on all ESXi hosts where the underlying servers support UEFI secure boot. You should also gather encryption recovery information from all ESXi hosts that use UEFI secure boot mode and securely save the encryption recovery information away.

Follow the example below to make sure ESXi host is using the TPM mode and secure boot is required. If the Mode output is None, update the mode parameter to use TPM encryption mode, set the require-secure-boot parameter to true, and then check the settings again.

```
[root@esxi-a-03:~] esxcli system settings encryption get
Mode: NONE
Require Executables Only From Installed VIBs: false
Require Secure Boot: false

[root@esxi-a-03:~] esxcli system settings encryption set --mode=TPM

[root@esxi-a-03:~] esxcli system settings encryption set --require-secure-boot=T

[root@esxi-a-03:~] esxcli system settings encryption get
```

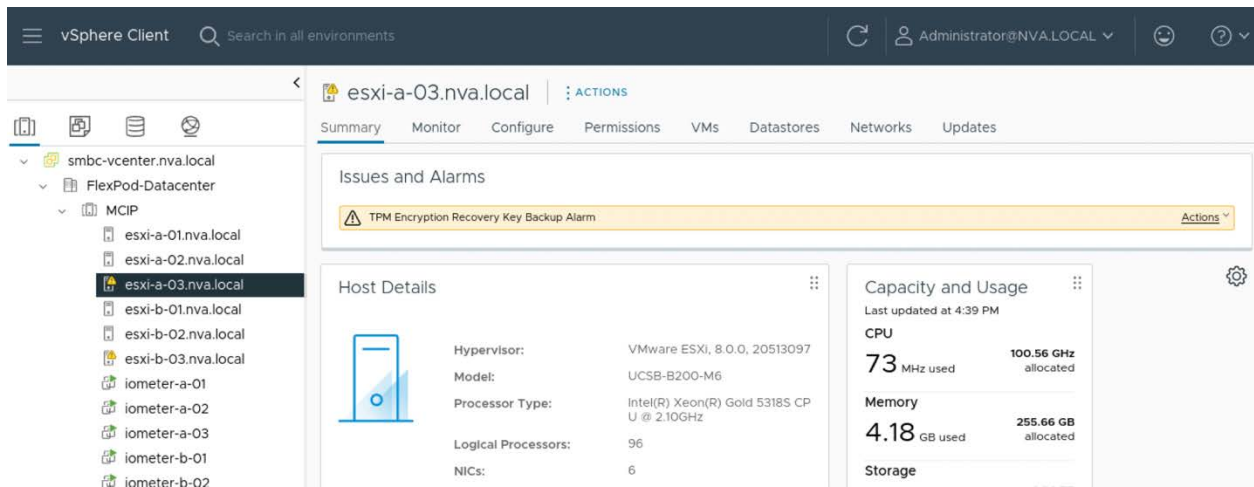
```
Mode: TPM
Require Executables Only From Installed VIBs: false
Require Secure Boot: true
```

The secure boot encryption recovery information is required to properly boot an ESXi server again after associating its service profile with a different underlying physical server hardware after a hardware replacement.

To gather the recovery information from all ESXi hosts using UEFI secure boot, log in to the hosts as the root user, list the encryption recovery information, and securely save the Recovery ID and Key information for all ESXi hosts.

```
[root@esxi-a-03:~] esxcli system settings encryption recovery list
Recovery ID                               Key
-----
{F7CFD208-E7C7-4D50-8AA9-A32E2064994B}  331342-134993-057950-232411-709944-082109-239663-322153-
288450-105147-192004-074723-523744-409928-597006-546946
```

Please note that vCenter Server issues alarms for hosts with TPM mode enabled. You can use the Reset to Green under Actions drop-down list to acknowledge the alarm after securely backed up the encryption recovery information from all hosts for future recovery purposes.



NFS access authorization

Layered access configuration overview

There are several layers of configurations that will be needed within the various components of a FlexPod virtual infrastructure solution to provide NFS protocol data services. Here are highlights of some of the needed configurations.

- NFS VLAN will need to be properly configured in all Nexus switches, in UCS Manager VLAN networking, and for ONTAP storage data ports.
- The ONTAP storage virtual machine (SVM) providing the NFS protocol service must have the NFS protocol enabled and NFS LIFs configured.
- If switch ACL is in use for the NFS VLAN, then the IPs of the ESXi NFS vmkernel ports and the NFS LIFs of the ONTAP storage cluster must be allowed to access the NFS VLAN.
- The ONTAP SVM must have the NFS volume created and exported, and the SVM export policy must allow access from the ESXi hosts' NFS vmkernel ports.
- ESXi hosts must be configured to mount the NFS volume from the configured junction-path of the exported NFS volume.

ONTAP export policy

ONTAP uses export policy to permit client access to NFS volumes. An export policy works very much like the access control list on the Nexus switches. The ONTAP NFS export policy contains one or more export rules, and the policy can be associated with a volume to configure client access to the volume. The result of this rule-checking process determines whether a client is granted or denied (with a permission-denied message) access to the volume.

When a new storage virtual machine (SVM) is created, a default export policy (called default) is created automatically. You must create one or more rules for the default export policy before clients can access data on the SVM. You should verify that access is open to all NFS clients in the default export policy, and later restrict access to individual volumes by creating custom export policies for individual volumes as necessary.

The following example illustrates the commands for showing the export-policy of the infrastructure SVM, creating an export-policy rule for NFS clients using a subnet matching approach, showing the created export-policy rule, and assigning the export policy to the root volume of the SVM.

```
SiteA::> vserver export-policy show -vserver Infra_SiteA -policyname default

Vserver: Infra_SiteA
Policy Name: default

SiteA::> vserver export-policy rule create -vserver Infra_SiteA -policyname default -ruleindex 1
-protocol nfs -clientmatch 172.21.79.0/24 -rorule sys -rwrule sys -superuser sys -allow-suid true

SiteA::> vserver export-policy rule show -vserver Infra_SiteA -policyname default
```

Vserver	Policy Name	Rule Index	Access Protocol	Client Match	RO Rule
Infra_SiteA	default	1	nfs	172.21.79.0/24	sys

```
SiteA::> volume modify -vserver Infra_SiteA -volume Infra_SiteA_root -policy default
Volume modify successful on volume Infra_SiteA_root of Vserver Infra_SiteA.
```

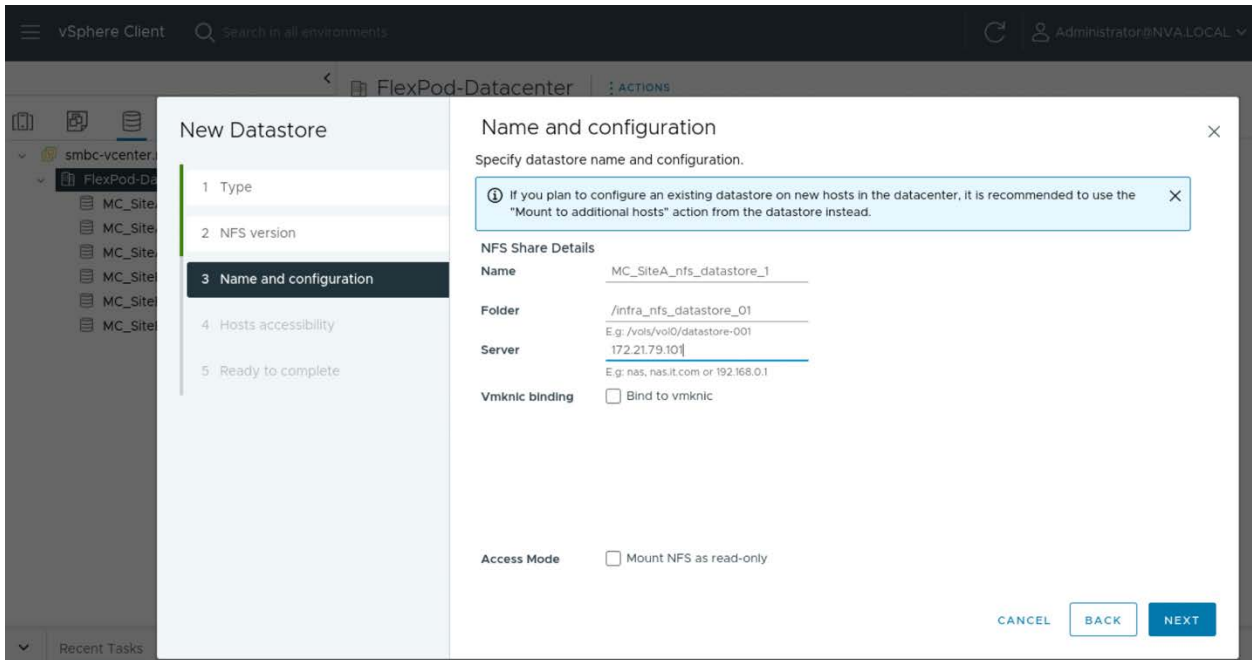
Note: Using the entire NFS subnet for the export-policy rule simplifies NFS client access configuration. However, if individual NFS client IP match is desirable due to security consideration, then IP address of the individual client should be provided to the `-clientmatch` parameter. Additional export-policy rules will need to be added to allow additional NFS clients to access the volume.

The following example shows how you can create a thin-provisioned 1TB volume in ONTAP and prepare it for export from the designated junction-path `/infra_nfs_datastore_01`.

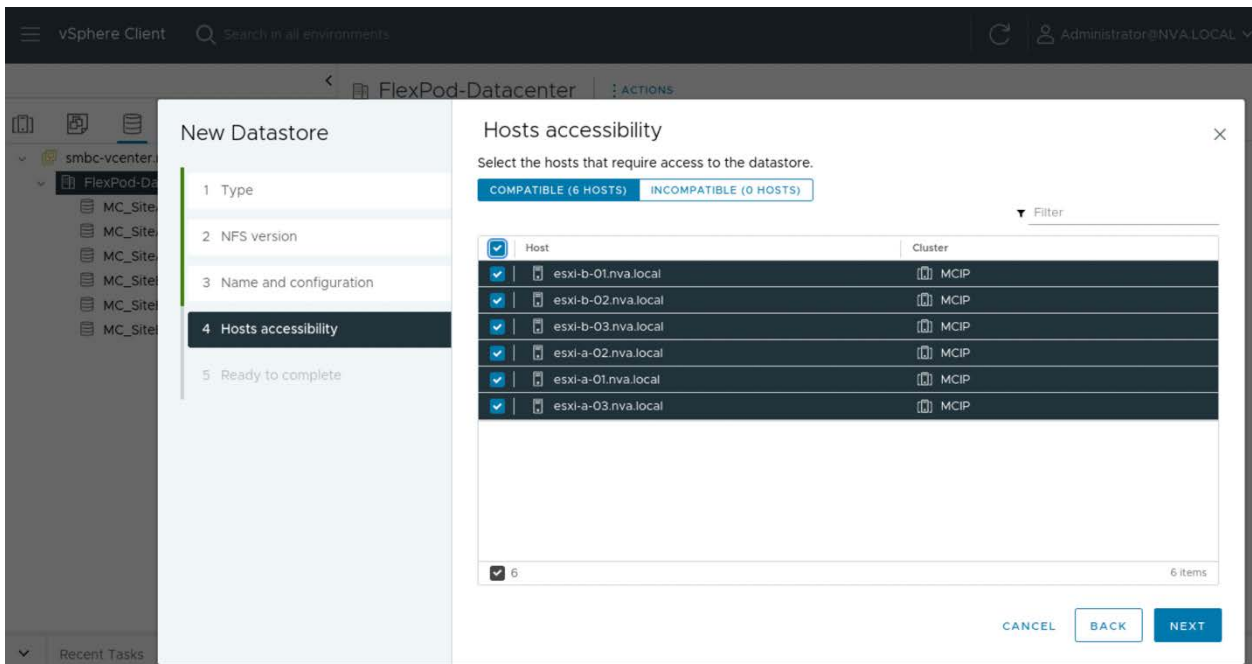
```
volume create -vserver Infra_SiteA -volume infra_nfs_datastore_01 -aggregate aggr1_SiteA_03 -size 1TB -state online -policy default -junction-path /infra_nfs_datastore_01 -space-guarantee none -percent-snapshot-space 0
```

Mount NFS volume in VMware

From VMware vCenter Server, you can mount the newly exported NFS volume by invoking the New Datastore configuration dialog. You go through the datastore type and NFS protocol version selections, provide the datastore name and configuration details, and select the hosts that require access to the datastore as shown in the screenshots below.



Note: The Folder name is the junction-path of the exported NFS volume from the volume creation command. The Server address is the NFS LIF address of the ONTAP cluster node which is hosting the exported volume.



Kerberos considerations

If Kerberos is used in your environment for strong authentication, you need to work with your Kerberos administrator to determine requirements and appropriate storage system configurations, and then enable the SVM as a Kerberos client. In addition, the environment requires DNS, NTP, and a secure directory service such as Active Directory, or OpenLDAP configured to use LDAP over SSL/TLS.

Also, if Kerberos authentication is required, select NFSv4 or later version to fully realize the security benefits of Kerberos in ONTAP. When Kerberos is enabled on the SVM, be sure to enable Kerberos on several data LIFs on multiple nodes for redundancy and use one of the three available security methods: krb5 (Kerberos 5 protocol), krb5i (Kerberos v5 protocol with integrity checking using checksums), or krb5p (Kerberos v5 protocol with privacy service).

ONTAP data-at-rest encryption

Data-at-rest encryption is important to protect sensitive data in the event a storage system is stolen, repurposed, or returned. ONTAP 9 has three FIPS 140-2 compliant data-at-rest encryption solutions:

- NetApp Storage Encryption (NSE) is a hardware solution that uses self-encrypting drives (SEDs).
- NetApp Aggregate Encryption (NAE) is a software solution that enables encryption of any data volume on any drive type where it is enabled with unique keys for each aggregate.
- NetApp Volume Encryption (NVE) is a software solution that enables encryption of any data volume on any drive type where it is enabled with a unique key for each volume.

With NSE, full disk encryption is available with FIPS 140-2 level 2 SEDs. Full disk encryption is also available for NVMe SEDs that do not have FIPS 140-2 certification.

NSE, NAE, and NVE can use either external key management or the onboard key manager (OKM). Use of NSE, NAE, and NVE does not affect ONTAP storage efficiency features. NAE volumes participate in and benefit from aggregate deduplication. However, NVE volumes are excluded from aggregate deduplication.

If you need to segregate access to data and make sure that data is protected all the time, NSE SEDs can be combined with network- or fabric-level encryption. NSE SEDs act like a backstop if an administrator forgets to configure or misconfigures higher-level encryption. By using both software (NAE or NVE) and hardware (NSE or NVMe SED) you can achieve double encryption at rest.

Note: You can check on NetApp Hardware Universe, <https://hwu.netapp.com>, for the drive support details for your platform configuration and the running ONTAP release. The screenshot below shows the supported drives, including self-encrypting drives, for the AFF A250 MetroCluster IP solution's embedded shelf.

Supported Shelf Drives - AFF A250 with ONTAP 9.13.1

Platform Configuration: AFF A250 4-Node MetroCluster IP

Zero Embedded Drive Configuration

Supported Shelves DrivesSAS Shelf Mixing and Stacks data

Part No.	Capacity	RPM	Drive Type	Encryption	Root-Data Partitioning	Root-Data-Data Partitioning	Storage Pool Partitioning	Max Drive Count	Max Stack Size	FlexArray	Drive Strings	EOA	EOS
AFF A250-4NMCIP Internal Drives													
X4010A	1920GB	N/A	NVMe SSD	AES-256	No	Yes	No	48	N/A	No	View		
X4011A	3840GB	N/A	NVMe SSD	AES-256	No	Yes	No	48	N/A	No	View		
X4012A [1]	3840GB	N/A	NVMe SSD	AES-256, FIPS 140-2 Level 2, NSE	No	Yes	No	48	N/A	No	View		
X4013A	7680GB	N/A	NVMe SSD	AES-256	No	Yes	No	48	N/A	No	View		
X4014A	15300GB	N/A	NVMe SSD	AES-256	No	Yes	No	48	N/A	No	View		
X4016A	3840GB	N/A	NVMe SSD	No	No	Yes	No	48	N/A	No	View		
X4018A	1920GB	N/A	NVMe SSD	No	No	Yes	No	48	N/A	No	View		
X4019A [1]	15300GB	N/A	NVMe SSD	AES-256, FIPS 140-2 Level 2, NSE	No	Yes	No	48	N/A	No	View		

ONTAP data-in-flight encryption

ONTAP IPsec data-in-flight encryption

Internet Protocol Security (IPsec) is an IETF standard. ONTAP uses IPsec in transport mode to ensure data is continuously secure and encrypted, even while in transit. ONTAP IPsec provides end-to-end encryption support for all IP traffic between a client and an ONTAP SVM. IPsec data encryption for all IP traffic includes support for NFS, iSCSI, and SMB/CIFS protocols. After IPsec is configured, network traffic

between the client and ONTAP is protected with preventive measures to combat replay and man-in-the-middle (MITM) attacks.

Providing NFS encryption over the wire is one of the main use cases for IPsec. Prior to ONTAP 9.8, NFS over-the-wire encryption required the setup and configuration of Kerberos to utilize krb5p to encrypt NFS data in flight. This is not always simple or easy to accomplish in every customer environment.

You can check if IPsec is enabled on the cluster and enable it to ensure data is continuously secure and encrypted, even while in transit, as shown in the following example.

```
SiteA::> security ipsec config show
    IPsec Enabled: false
    IPsec Log Level: 2
    Replay Window Size: 0

SiteA::> security ipsec config modify -is-enabled true

SiteA::> security ipsec config show
    IPsec Enabled: true
    IPsec Log Level: 2
    Replay Window Size: 0
```

Although the IPsec capability must be enabled on the cluster, it applies to individual SVM IP addresses using a Security Policy Database (SPD) entry. The policy (SPD) entry contains the client IP address (remote IP subnet), SVM IP address (local IP subnet), the encryption cipher suite to use, and the pre-shared key (PSK). In addition to the IPsec policy entry, the client must be configured with the same information (local and remote IP, PSK, and cipher suite) before traffic can flow over the IPsec connection.

Note: For NetApp SnapMirror and cluster peering traffic encryption, cluster peering encryption (CPE) is still recommended over IPsec for secure in-transit over the wire. CPE performs better for these workloads than IPsec. You do not need a license for IPsec, and there are no import or export restrictions.

Note: See the ONTAP 9 Network Management documentation for more information about IPsec.

ONTAP cluster peering encryption

You can protect your data by replicating it to a remote cluster for data backup and disaster recovery purposes with features such as SnapMirror and SnapVault®. The clusters must be in a peer relationship so that they can communicate with each other and perform the data mirroring. The source cluster and destination cluster use inter-cluster network interfaces to communicate with each other and to exchange data.

New cluster-peer relationships established with ONTAP 9.6 and later have cluster peering encryption (CPE) enabled by default. CPE uses a PSK and the Transport Layer Security (TLS) to secure cross-cluster peering communications. Cluster peering encrypts all data between the cluster peers. For example, when using SnapMirror, all peering information as well as all SnapMirror relationships between the source and destination cluster peer are encrypted. This adds an additional layer of security between the peered clusters.

To check if CPE is enabled, issue the `cluster peer show` command to examine the encryption setting. As shown in the example below, `tls-psk` is the encryption protocol used for inter-cluster communication.

```
SiteA::> cluster peer show -instance

    Peer Cluster Name: SiteB
    Remote Intercluster Addresses: 172.21.84.201, 172.21.84.202
    Availability of the Remote Cluster: Available
    Remote Cluster Name: SiteB
    Active IP Addresses: 172.21.84.206, 172.21.84.207
    Cluster Serial Number: 1-80-000011
    Remote Cluster Nodes: SiteB-03, SiteB-04
```

```
Remote Cluster Health: true
Unreachable Local Nodes: -
Address Family of Relationship: ipv4
Authentication Status Administrative: use-authentication
Authentication Status Operational: ok
Last Update Time: 10/8/2023 11:50:50
IPspace for the Relationship: Default
Proposed Setting for Encryption of Inter-Cluster Communication: -
Encryption Protocol For Inter-Cluster Communication: tls-psk
Algorithm By Which the PSK Was Derived: jpake
```

Note: To enable encryption on cluster peer relationships that were created before ONTAP 9.6, you must first upgrade the source and destination cluster to 9.6 and later and then use the `cluster peer modify` command to change both the source and destination cluster peers to use cluster peering encryption. For more information about cluster peering encryption, see the Cluster and SVM peering information in the ONTAP 9 documentation.

ONTAP ransomware protection

Ransomware attacks continue to be big threats to enterprises as attacks can potentially lead to business disruptions, monetary and data losses, and business reputation impacts. NetApp provides a suite of tools and solutions that can be utilized to help detect and recover from ransomware attacks quickly to minimize business impacts.

The ONTAP FPolicy framework is used to monitor and manage file access. ONTAP volume Snapshot is a point-in-time copy of the volume data for quick recovery. Autonomous ransomware protection (ARP) automates the detection and provides protection and alerts for ransomware attacks. Additional external tools such as NetApp Cloud Insights can help make the orchestration and protection against ransomware simple.

FPolicy

NetApp FPolicy is a file access notification framework that is used to monitor and manage file access events on storage virtual machines (SVMs) through native or partner solutions. There are two parts to an FPolicy solution. The first part of the solution is the ONTAP framework which contains and maintains the FPolicy configuration, monitors file events, and sends notifications to native or external FPolicy servers. The second part of the solutions is the native or external FPolicy servers which process notifications sent by ONTAP FPolicy to fulfill customer use cases such as data governance, compliance, and ransomware protection.

FPolicy determines how the storage system handles requests from individual client systems for operations such as create, open, rename, and delete. There are two basic FPolicy configuration types. One configuration uses external FPolicy servers, such as NetApp Cloud Insights, to process and act upon notifications. The other configuration uses the ONTAP native FPolicy server for simple file blocking based on extensions.

For example, an administrator can configure FPolicy to scan for files based on the following to avoid storing mp3 file types on the system:

- File extensions (natively supported in ONTAP): For example, block all files matching *.mp3. This is a fast but less reliable approach. Native support for file blocking based on file extensions does not require a connection to any external FPolicy server.
- File signatures (requires external FPolicy server): For example, block all files with signature matching mp3 format. This approach is slower as the FPolicy server needs to access the data in the file. However, this approach is more accurate as signature matching is performed.

The administrator should enable events for CREATE, OPEN, CLOSE and RENAME requests. When the FPolicy server is notified of these event triggers, it can run checks based on either of the two mechanisms (file extension or file signature) and DENY requests if a match is found.

The external FPolicy notifications are sent either in synchronous or asynchronous mode. With asynchronous notifications, the node does not wait for a response. Asynchronous notification is suitable for applications where the FPolicy server does not require that actions be taken because of notification evaluation such as for the monitoring and auditing of the file access activities. With synchronous notifications, the FPolicy server must acknowledge every notification. Synchronous notification is used when an action is required based on the results of notification evaluation such as deciding whether to allow or deny requests based on criteria specified on the external FPolicy server.

Volume Snapshot and policy

A Snapshot copy is a read-only, point-in-time image of a volume. A Snapshot copy consumes minimal storage space and incurs negligible performance overhead. You can use a Snapshot copy to restore the entire contents of a volume, or to recover individual files or LUNs. Snapshot copies are stored in the .snapshot directory on the volume.

A Snapshot policy defines how the system creates Snapshot copies. The policy specifies when to create Snapshot copies, how many copies to retain, and how to name them. The default policy for a volume automatically creates Snapshot copies based on the following schedule, with the oldest Snapshot copies deleted to make room for newer copies:

- A maximum of six hourly Snapshot copies taken five minutes past the hour.
- A maximum of two daily Snapshot copies taken Monday through Saturday at 10 minutes after midnight.
- A maximum of two weekly Snapshot copies taken every Sunday at 15 minutes after midnight.

You can examine the default snapshot policy as shown in the example below.

```
SiteA::> snapshot policy show -policy default
Vserver: SiteA
```

Policy Name	Number of Is					
	Schedules	Enabled	Comment			
default	3	true	Default policy with hourly, daily & weekly schedules.			
Schedule	Count	Prefix	SnapMirror Label	Retention Period		
hourly	6	hourly	-	0 seconds		
daily	2	daily	daily	0 seconds		
weekly	2	weekly	weekly	0 seconds		

Unless you specify a Snapshot policy when you create a volume, the volume inherits the Snapshot policy associated with its containing storage virtual machine (SVM).

The following example creates a job schedule to run every 15 minutes, creates a Snapshot policy named snap_policy_custom, and applies the policy to a specific volume. The created Snapshot policy includes weekly, daily, hourly, and the new 15-minute schedules, each specified with the maximum number of copies, and the snapshot name prefix.

```
SiteA::> job schedule interval create -name 15min -minutes 15

SiteA::> volume snapshot policy create -vserver Infra_SiteA -policy snap_policy_custom -schedule1
weekly -prefix1 weekly -count1 2 -schedule2 daily -prefix2 daily -count2 2 -schedule3 hourly -
prefix3 hourly -count3 6 -schedule4 15min -prefix4 15min -count4 8 -enabled true

SiteA::> volume modify -vserver Infra_SiteA -volume Infra_SiteA_datastore_1 -snapshot-policy
snap_policy_custom

Warning: You are changing the Snapshot policy on volume "Infra_SiteA_datastore_1" to
"snap_policy_custom". Snapshot copies on this volume that
do not match any of the prefixes of the new Snapshot policy will not be deleted.
However, when the new Snapshot policy takes effect,
depending on the new retention count, any existing Snapshot copies that continue to use
the same prefixes might be deleted. See the
'volume modify' man page for more information.
```

```
Do you want to continue? {y|n}: y
Volume modify successful on volume Infra_SiteA_datastore_1 of Vserver Infra_SiteA.
```

After sufficient time has passed, there should be Snapshots created based on configured Snapshot schedules. As the following example output shows, there are eight 15min Snapshots, six hourly Snapshots, two daily Snapshots, and two weekly Snapshots available.

```
SiteA::> snapshot show -vserver Infra_SiteA -volume Infra_SiteA_datastore_1
---Blocks---
Vserver  Volume      Snapshot                                     Size Total% Used%
-----
Infra_SiteA
  Infra_SiteA_datastore_1
    weekly.2023-10-01_0015                    3.38GB      0%    1%
    weekly.2023-10-08_0015                    2.90GB      0%    1%
    daily.2023-10-12_0010                    2.09GB      0%    1%
    daily.2023-10-13_0010                   18.49MB      0%    0%
    hourly.2023-10-13_1005                    5.85MB      0%    0%
    hourly.2023-10-13_1105                    6.05MB      0%    0%
    hourly.2023-10-13_1205                     7MB         0%    0%
    hourly.2023-10-13_1305                    3.86MB      0%    0%
    15min.2023-10-13_1322                     3.34MB      0%    0%
    15min.2023-10-13_1337                     3.43MB      0%    0%
    15min.2023-10-13_1352                     3.07MB      0%    0%
    hourly.2023-10-13_1405                    1.51MB      0%    0%
    15min.2023-10-13_1407                     4.29MB      0%    0%
    15min.2023-10-13_1422                     3.95MB      0%    0%
    15min.2023-10-13_1437                     3.27MB      0%    0%
    15min.2023-10-13_1452                     3.29MB      0%    0%
    hourly.2023-10-13_1505                    1.29MB      0%    0%
    15min.2023-10-13_1507                    5.65MB      0%    0%
18 entries were displayed.
```

With ONTAP release 9.12.1 and later, you can also lock a Snapshot copy on a non- SnapLock® volume. Locking Snapshot copies ensures that they can't be deleted accidentally or maliciously.

Autonomous ransomware protection

In addition to ransomware detection and prevention using external FPolicy user behavioral analytics (UBA) with NetApp Cloud Insights and the NetApp FPolicy partner ecosystem, ONTAP 9.10.1 introduces autonomous ransomware protection. ONTAP anti-ransomware uses a built-in on-box machine learning (ML) capability that looks at NAS (NFS and SMB) volume workload activity plus data entropy to automatically detect ransomware. It monitors for activity that is different from UBA so that it can detect attacks that UBA does not.

When you enable autonomous ransomware protection (ARP), it runs in learning mode. In learning mode, the ONTAP system develops an alert profile based on the analytic areas: entropy, file extension types, and file IOPS. After running ARP in learning mode for enough time to assess workload characteristics, you can switch to active mode and start protecting your data. Once ARP has switched to active mode, ONTAP will create ARP snapshots to protect the data if a threat is detected.

Although you can switch from learning mode to active mode at any time, it is recommended that you leave ARP in learning mode for a minimum of 30 days. Switching to active mode too early might lead to too many false positives. Beginning with ONTAP 9.13.1, ARP automatically determines the optimal learning period interval and automates the switch, which may occur before 30 days.

For more detailed information about this capability, see [TR-4572: The NetApp solution for ransomware](#), [TR-4961: FlexPod ransomware protection & recovery with NetApp Cloud Insights and SnapCenter](#), and [ONTAP autonomous ransomware protection overview](#).

Note: ARP is now part of the ONTAP One license and available to all customers.

SnapLock protection / compliance

ONTAP SnapLock® is a high-performance compliance solution that provides capability of data retention and WORM protection for retained data. You can use SnapLock to create non-modifiable and non-erasable volumes to prevent files from being altered or deleted until a set retention date.

SnapLock allows this retention to be performed at the file level through standard open file protocols such as CIFS and NFS. The supported open file protocols for SnapLock are NFS (versions 2, 3, and 4) and CIFS (SMB 1.0, 2.0, and 3.0).

SnapLock WORM storage uses NetApp Snapshot technology and can leverage SnapMirror replication, and SnapVault backups as the base technology for providing backup recovery protection for data.

You use the SnapLock compliance clock feature to lock Snapshot copies for a specified period so that they cannot be deleted until the expiration time is reached. Locking Snapshot copies makes them tamperproof and protecting them from ransomware threats. You can use locked Snapshot copies to recover data if a volume is compromised by a ransomware attack.

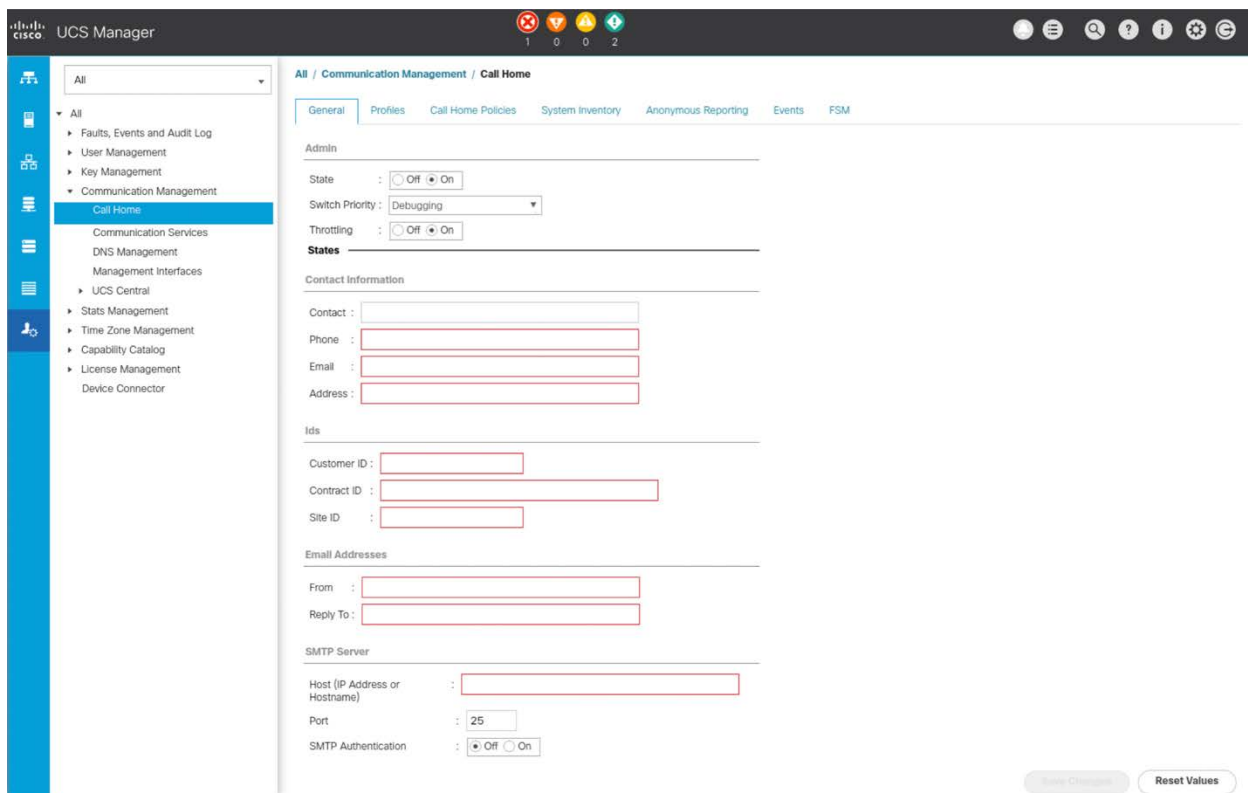
Support information

Cisco UCS Call Home

Cisco UCS Call Home can deliver alert messages containing diagnostics, environmental faults, and event information. You can use the Call Home feature to email a network operations center, page a support engineer, or use Cisco Smart Call Home services to open a case with the Technical Assistance Center (TAC). A range of message formats are available for compatibility with XML-based automated parsing applications or pager services.

It is highly recommended by Cisco to configure Call Home in Cisco UCS Manager. Configuring Call Home will accelerate the resolution of support cases. You can configure UCS Call Home by going over the following steps.

Log in to Cisco UCS Manager, select Admin menu, expand All > Communication Management, and select Call Home. Under General tab, change the Admin State to On, fill in contact information, IDs, email addresses, and SMTP server information. Finally, click Save Changes and Ok to complete the UCS Call Home configuration.



Cisco Nexus Smart Call Home

Cisco Nexus Smart Call Home provides an email-based notification for critical system policies. You can use the Call Home feature to email a network operations center, page a support engineer, or use Cisco Smart Call Home services to open a case with the Technical Assistance Center (TAC).

Smart Call Home provides secure message transport from devices, continuous device health monitoring and real-time diagnostics alerts, Smart Call Home message analysis. It facilitates automatic execution and attachment of relevant CLI command output to speed up issue resolution. It supports multiple message formats, such as short text, full text, and XML formats to serve different communication needs.

To register for Smart Call Home, you will need your SMARTnet contract and your contact information. Please refer to the Cisco Nexus Smart Call Home documentation for details on the pre-requisites, configuration details, and the supported alert group and command output collection information.

NetApp ONTAP support information

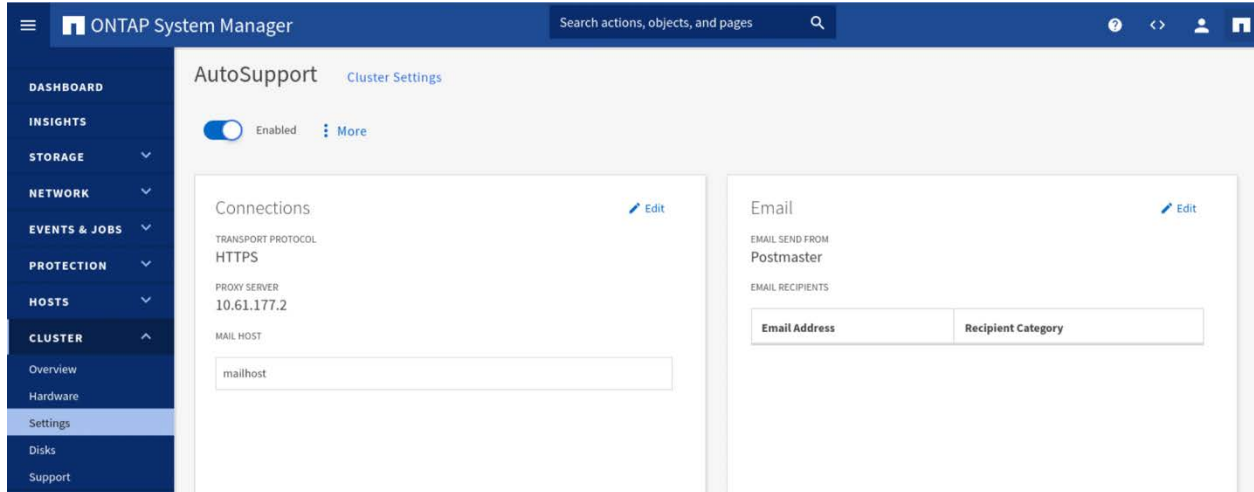
ONTAP AutoSupport® is a mechanism that proactively monitors the health of your ONTAP system and automatically sends messages to NetApp technical support, your internal support organization, or a support partner.

The AutoSupport component of ONTAP collects telemetry data and sends it for analysis. Active IQ Digital Advisor analyzes the data from AutoSupport and provides proactive care and optimization. Using artificial intelligence, Active IQ can identify potential problems and help you resolve them before they impact your business. By default, the system collects AutoSupport information and stores it locally, even if you disable AutoSupport. While you can disable AutoSupport at any time, you should leave it enabled.

While AutoSupport messages to technical support are enabled by default, you must set the correct options and have a valid mail host to have messages sent to your internal support organization. Only the

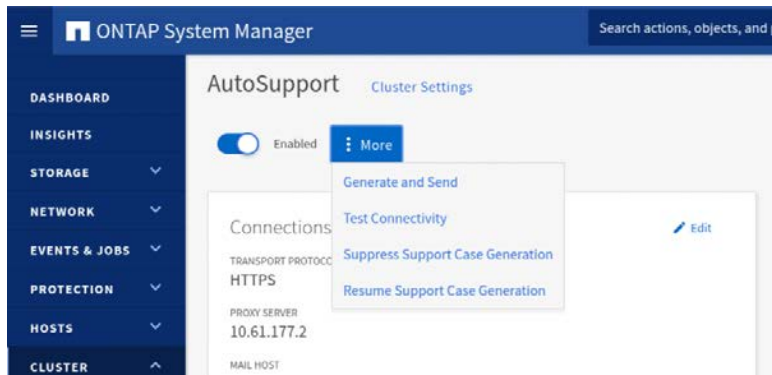
cluster administrator can perform AutoSupport management. The storage virtual machine (SVM) administrator has no access to AutoSupport.

To configure AutoSupport from the ONTAP System Manager, go to Cluster > Settings, click on the ellipsis in the AutoSupport tile, select More options to configure the settings for AutoSupport, such as transport protocol, proxy server, mail host, email sender and recipients.



Note: The HTTPS transport protocol is the default and the recommend protocol for sending AutoSupport.

In addition to automatically generated AutoSupport, you can also generate AutoSupport on demand by clicking on the ellipsis and select Generate and Send action.



VMware support information

ESXi diagnostic information

When you submit a support request with VMware Technical Support, you will typically be asked to provide diagnostic information from your ESXi hosts. The diagnostic information for ESXi hosts can be gathered by using the `vm-support` script available on ESXi hosts. The following example illustrates how you can use `vm-support` command to create a diagnostic bundle. At the end of the execution, the script shows you the location of the collected diagnostic information file.

```
[root@esxi-b-01:~] vm-support
/bin/vm-support v4.1: 17:27:17, action threads 4
17:27:44: Gathering output from sh -c DDIR=$(/usr/lib/vmware/vm-support/bin/find-datafile.py -ds
esx/cluster_agent_data/etcdData) && /bin/du $17:27:44: Gathering output from /sbin/vsi_traverse -
```

```

s |
17:28:39: Gathering output from /usr/lib/vmware/vm-support/bin/dump-vmrk-rdm-info.sh
/vmfs/volumes/63390c86-2b4183b8-8bb6-0025b5f9a000/vdbench17:28:39: Gathering output from
vmkfstools -P -v 10 /vmfs/volumes/BOOTBANK1
17:28:39: Gathering output from /usr/lib/vmware/vm-support/bin/dump-vmrk-rdm-info.sh
/vmfs/volumes/63390bca-936ed95e-0a66-0025b5f9a000/vdbench17:28:39: Gathering output from
vmkfstools -P -v 10 /vmfs/volumes/61d06f2f-2d0c649e-7891-0025b5f7a000
...

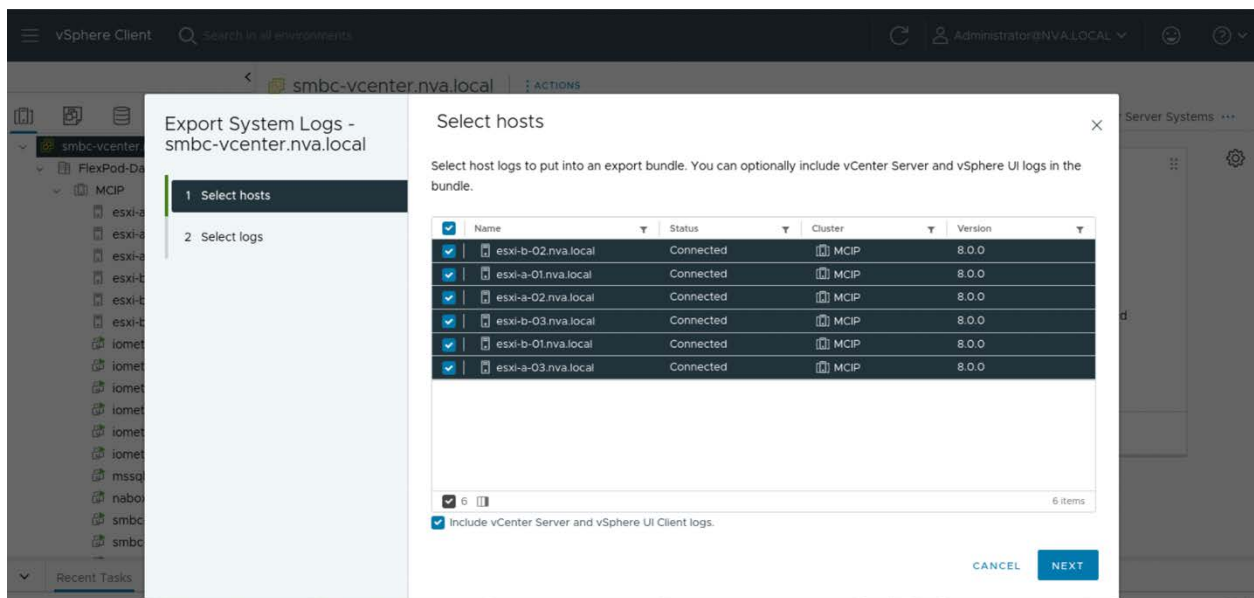
17:30:02: Gathering output from python ++group=vmsupport
/usr/lib/vmware/vsan/esxcli/esxcli_vsan_debug.py objects.overview --pyprint --vmsupp17:30:02:
Gathering output from python ++group=vmsupport /usr/lib/vmware/vsan/esxcli/esxcli_vsan_debug.py
objects.info --pyprint --vmsupport 17:30:02: Gathering output from /sbin/vdq -q -H
17:30:05: Done.
Please attach this file when submitting an incident report.
To file a support incident, go to http://www.vmware.com/support/sr/sr\_login.jsp
To see the files collected, check '/vmfs/volumes/63390c86-2b4183b8-8bb6-0025b5f9a000/esx-esxi-b-
01.nva.local-2023-10-24--17.27-39213415.tgz'

```

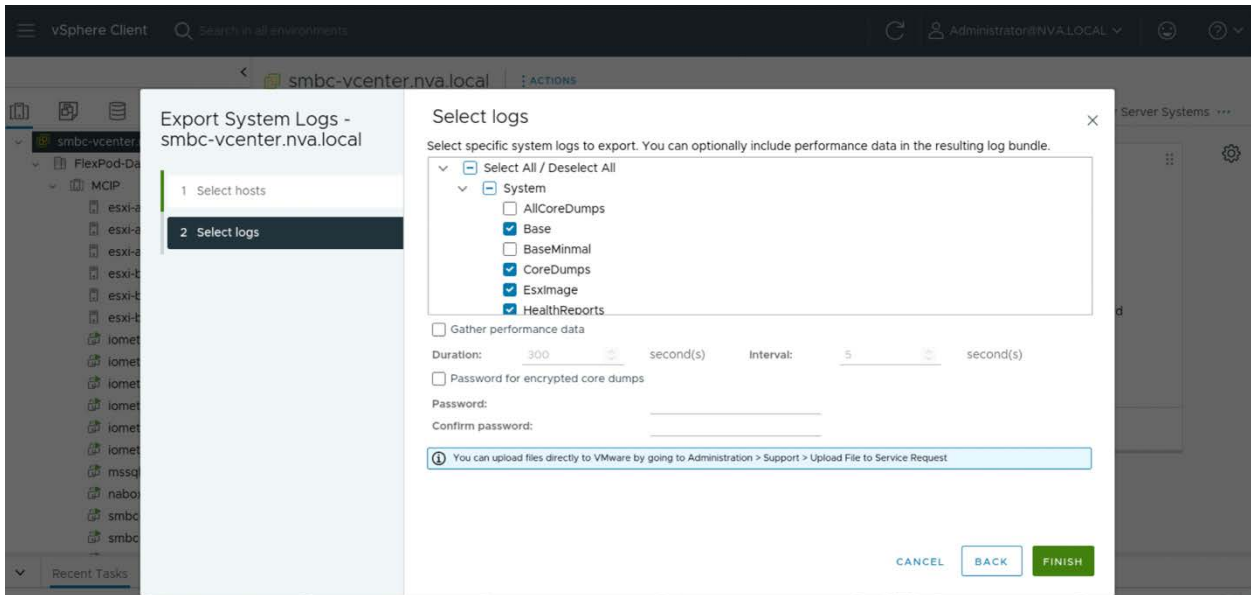
vCenter server diagnostic information

You can use VMware vCenter Server to collect diagnostic information for your cluster of ESXi hosts by using the Export System Logs action. You can optionally include the vCenter Server and vSphere UI Client logs, choose specific system logs to include, and gather performance data.

To gather vCenter Server diagnostic information, log in to vCenter Server through vSphere Client, select the vCenter Server object, right click the object for the Actions menu, and select the Export System Logs action. On the Select hosts dialog, specify the hosts logs to include, check to include vCenter Server and vSphere UI Client logs, and click Next.



On the Select logs dialog, you can select specific logs to export, check to include performance data, provide a password to encrypt the core dump, and then click Finish to generate the log bundle.



Security advisories

FlexPod converged infrastructure integrates solutions from NetApp, Cisco, and VMware. To provide a secure environment for your solutions, you need to follow security best practices for the respective components when deploying the solution. In addition, solution security is not a one-and-done effort. As new vulnerabilities are detected, companies make assessments on their products and provide security advisories to inform their customers on those issues as well as documenting fixes and workarounds. As an on-going security hardening effort, it is important to subscribe to security advisories from NetApp, Cisco, and VMware, evaluate those vulnerabilities, and apply remediations as appropriate to keep your FlexPod solution secure.

Cisco security advisories

Cisco Security Advisories are available on Cisco security information site, <https://sec.cloudapps.cisco.com/security/center/home.x>. On the Security Advisories page, you can review a list of vulnerability announcements and remediation instructions published by Cisco.

← → ↻ <https://sec.cloudapps.cisco.com/security/center/publicationListing.x> 90% ☆ ⓘ ⌵ ⌵ ⌵ ⌵

cisco Products Support & Learn Partners Events & Videos 🔍 👤 🌐 US EN

Home / Cisco Security / Security Advisories

Cisco Security
Cisco Security Advisories

Vulnerabilities Filter By Product

Quick Search 🔍 [Advanced Search](#)

ADVISORY	IMPACT ⓘ	CVE	LAST UPDATED ⓘ	VERSION
Search Advisory Name	All ▼	Search CVE	Most Recent ▼	
▶ Cisco IOS XR Software Image Verification Vulnerability	Medium	CVE-2023-20135	2023 Sep 13	1.0
▶ Cisco IOS XR Software IPXE Boot Signature Bypass Vulnerability	Medium	CVE-2023-20236	2023 Sep 13	1.0
▶ Cisco IOS XR Software Connectivity Fault Management Denial of Service Vulnerability	Medium	CVE-2023-20233	2023 Sep 13	1.0

To find the security advisories for a particular Cisco product of interest, e.g., Cisco Unified Computing System (Management Software) and Cisco NX-OS Software, click on the Filter By Product tab, select the products, and set Apply to filter on those products as shown below.


Cisco Security
Cisco Security Advisories

Vulnerabilities **Filter By Product**

Remove All 🗑️

Cisco Unified Computing System (Mana ▼
☐ Apply ☒

Cisco NX-OS Software ▼
☐ Apply ☒







Add a Product

[Advanced Search](#)

ADVISORY	IMPACT ⓘ	CVE	LAST UPDATED ⓘ	VERSION
Search Advisory Name	All ▼	Search CVE	Most Recent ▼	
▶ Cisco Nexus 3000 and 9000 Series Switches SFTP Server File Access Vulnerability	Medium	CVE-2023-20115	2023 Aug 23	1.0
▶ Cisco NX-OS Software TACACS+ or RADIUS Remote Authentication Directed Request Denial of Service Vulnerability	High	CVE-2023-20168	2023 Aug 23	1.0
▶ Cisco Nexus 3000 and 9000 Series Switches IS-IS Protocol Denial of Service Vulnerability	High	CVE-2023-20169	2023 Aug 23	1.0

As illustrated in the screenshots below, you can click on the arrow to the left of the Advisory Name to quickly see a summary of the security advisory, whether a workaround is available, or the publishing

information. You can click on the Advisory Name to see a full description of the security advisory, affected products, workarounds, fixed software, and find additional resources and information.

ADVISORY	IMPACT	CVE	LAST UPDATED	VERSION
<input type="text" value="Search Advisory Name"/>	All	<input type="text" value="Search CVE"/>	Most Recent	
<div><div></div><div>Cisco Nexus 3000 and 9000 Series Switches SFTP Server File Access Vulnerability</div></div> <div><div>Publication ID: cisco-sa-nxos-sftp-xVAp5Hfd</div><div>Version: 1.0</div><div>First Published: 2023 Aug 23 16:00 GMT</div></div> <div>Workaround: Yes</div> <div>Summary: A vulnerability in the SFTP server implementation for Cisco Nexus 3000 Series Switches and 9000 Series Switches in standalone NX-OS mode could allow an authenticated, remote attacker to download or overwrite files from the underlying operating system of an affected device. This Read More...</div>	Medium	CVE-2023-20115	2023 Aug 23	1.0
<div><div></div><div>Cisco NX-OS Software TACACS+ or RADIUS Remote Authentication Directed Request Denial of Service Vulnerability</div></div>	High	CVE-2023-20168	2023 Aug 23	1.0
<div><div></div><div>Cisco Nexus 3000 and 9000 Series Switches IS-IS Protocol Denial of Service Vulnerability</div></div>	High	CVE-2023-20169	2023 Aug 23	1.0
<div><div></div><div>Cisco NX-OS Software CLI Command Injection Vulnerability</div></div>	Medium	CVE-2023-20050	2023 Feb 22	1.0

Home / Cisco Security / Security Advisories

 Cisco Security Advisory

Cisco Nexus 3000 and 9000 Series Switches SFTP Server File Access Vulnerability



Advisory ID: cisco-sa-nxos-sftp-xVAp5Hfd CVE-2023-20115
First Published: 2023 August 23 16:00 GMT
Version 1.0: Final
Workarounds: Yes
Cisco Bug IDs: CSCwe47138
CVSS Score: Base 5.4

[Download CSAF](#)
[Download CVRF](#)
[Email](#)

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the [Security Vulnerability Policy](#). This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Subscribe to Cisco Security Notifications

[Subscribe](#)

Related to This Advisory

[Cisco Event Response: August 2023 Semiannual Cisco FXOS and NX-OS Software Security Advisory Bundled Publication](#)

Summary

A vulnerability in the SFTP server implementation for Cisco Nexus 3000 Series Switches and 9000 Series Switches in standalone NX-OS mode could allow an authenticated, remote attacker to download or overwrite files from the underlying operating system of an affected device.

This vulnerability is due to a logic error when verifying the user role when an SFTP connection is opened to an affected device. An attacker could exploit this vulnerability by connecting and authenticating via SFTP as a valid, non-administrator user. A successful exploit could allow the attacker to read or overwrite files from the underlying operating system with the privileges of the authenticated user.

Cisco has released software updates that address this vulnerability. There are workarounds that address this vulnerability.

This advisory is available at the following link:
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-sftp-xVAp5Hfd>

Under the Cisco Security Center Home page, <https://sec.cloudapps.cisco.com/security/center/home.x> , you can find additional security related information including Cisco policies and processes, Cisco security solutions, experts' blog, tactical resources, and notification registration for Cisco Security RSS feeds, Cisco Security Blog, and customized email notifications.

Cisco Intersight security advisories

Cisco Intersight is a Software-as-a-Service (SaaS) lifecycle management platform that simplifies infrastructure configuration, deployment, maintenance, and support. The platform significantly simplifies IT operations by bridging applications with infrastructure, providing visibility and management from bare-metal servers, hypervisors, to third-party storage systems deployed in the enterprise solution ecosystem.

In addition to the compute-specific hardware and software innovations, the integration of Cisco Intersight with Cisco UCS Manager, Cisco Nexus and MDS switches, NetApp Active IQ Unified Manager, and VMware vCenter Server delivers monitoring, orchestration, and workload optimization capabilities for FlexPod solutions.

For the on-going security monitoring, Intersight alerts users about the endpoint devices that are impacted by supported security advisories based on the versions running in the environment. You can click on the Advisories icon (loudspeaker icon) in the top menu bar in the dashboard to display the relevant Cisco Security Advisories.

The following is a partial screenshot of Advisories for the devices that have been claimed and discovered in the account. In the security advisories table, it provides description of the advisory, severity level, Common Vulnerabilities and Exposures (CVE) ID numbers, total number of affected devices, and the date and time of the update.

The screenshot shows the Cisco Intersight interface. The top navigation bar includes the Cisco logo, 'Intersight', a 'System' dropdown, a search bar, and notification icons for 19 alerts, 848 errors, and 1422 warnings. The left sidebar contains navigation links: Settings, Admin, Targets, Software Rep..., Tech Support, Audit Logs, Sessions, and Licensing. The main content area is titled 'Advisories' and has tabs for 'Security Advisories' (selected), 'Field Notices', 'End of Life Advisories', and 'Acknowledged'. A blue banner states: 'Advisories for affected devices only are listed here. For a complete list of advisories and more information, see [Help Center](#)'. Below this is a filter bar with '* All Security Adviso...' and an 'Add Filter' button. An 'Export' button and '13 items found' are also visible. The table has columns: Description, Severity, CVEs, Affected, and Last Update. The table lists four advisories:

Description	Severity	CVEs	Affected	Last Update
Intel 2023.1 IPU - BIOS and Processors Advisories	High	CVE-2022-373...	10	Aug 7, 2023 8:00 PM
Cisco FXOS Software and UCS Manager Software Configuration Backup Sta...	Medium	CVE-2023-20016	2	Mar 24, 2023 2:16 PM
Cisco Firepower 4100 Series, Firepower 9300 Security Appliances and UCS ...	Medium	CVE-2023-20015	2	Feb 22, 2023 11:00 AM
Intel 2023.1 IPU - BIOS Advisory	High	CVE-2022-263...	1	Feb 13, 2023 7:00 PM

To see the details of a particular advisory, you can simply click on the description link for it, such as the link for the [Intel 2023.1 IPU - BIOS Advisory](#) shown at the bottom of the screenshot above. The advisory page contains a summary of the advisory, links to the details on the Cisco security advisory portal, a list of the affected endpoint devices, workarounds, and the first fixed releases for the various server platform models. In addition, you can also acknowledge the advisory from the page by clicking on the Acknowledge button shown near the upper right-hand corner in the screenshot below.

Details

Severity

High

ID

Intel 2023.1 IPU - BIOS Advisory

CVEs

CVE-2022-26343,
CVE-2022-30539,
CVE-2022-32231, CVE-2022-26837,
CVE-2022-30704, CVE-2021-0187,
CVE-2022-36348,
CVE-2022-36794, CVE-2021-33124,
CVE-2022-21216, CVE-2022-33196,
CVE-2022-38090, CVE-2022-33972

Published

Feb 13, 2023 7:00 PM

Last Update

Feb 13, 2023 7:00 PM

Base Score

8.2

General

Intel 2023.1 IPU - BIOS Advisory

Summary

Potential security vulnerabilities in the BIOS firmware and Intel® Trusted Execution Technology (TXT) Secure Initialization (SINIT) Authenticated Code Modules (ACM) for some Intel® Processors may allow escalation of privilege. Intel is releasing BIOS updates to mitigate these potential vulnerabilities.

- CVE-2022-26343 impacts only M5 servers.
- CVE-2022-32231 impacts both M5 and M6 servers.
- Rest all CVEs impact only M6 servers.

Details

To learn more about the security vulnerability, the affected products, and other details, see:

- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00717.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00718.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00700.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00738.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00767.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00730.html>

Affected Devices (1)

 Advisories for the devices are processed every 3 hours. If you update the device, it can take up to 12 hours for the updated status to be displayed for the device. For more info see [Help Center](#)

1 items found 10 per page 1 of 1

Name	Type	Model / Type	Firmware / Version
site-b-fi-1-5	Server	UCSB-B200-M6	4.2(3c)

1 of 1

In the advisory page above, it shows that the B200 M6 server named site-b-fi-1-5 in our solution environment is affected by the advisory. Checking the UCS Manager equipment view as shown in the screenshot below, we can see that the affected server, Server 5, is not being used currently and does not have an associated service profile.

← → ↻ 🏠

🔒 🔍 📄 🌐

https://site-b-fi-vip.nva.local/app/ucsm/index.html#

☆

📧 ☰

Centos Wiki Documentation Forums

ucsm

UCS Manager

🔧 📄 📊 📉 📈

0 0 0 2

🔍 ⌵ 🔍 ? ⓘ ⚙️ ⌵

All

▼

▼ Equipment

▼ Chassis

▼ Chassis 1

► Fans

► IO Modules

► PSUs

▼ Servers

► Server 1

► Server 2

► Server 3

► Server 4

► Server 5

► Server 6

Equipment / Chassis / Chassis 1 / Servers

Servers

🔍 Advanced Filter ⬆ Export 🖨 Print

Name	Ov...	PID	Model	Se...	Profile	Us...	Co...	Co...	Th...	M...	Ad...	N/Cs	HB...	Op...	Po...	As...	Fa...
Server 1	🔴 ⬇	U...	Cisco UCS B200 M5 2 Socket...	FL...			20	20	40	13...	1	0	0	🟢 ⬆	🔴 ⬇	🔴 ⬇	N/A
Server 2	🟢 ⬆	U...	Cisco UCS B200 M5 2 Socket...	FL...	org-root/org-FlexPod-SMBC/its-VM-Host...		32	32	64	19...	1	6	0	🟢 ⬆	🟢 ⬆	🟢 ⬆	N/A
Server 3	🟢 ⬆	U...	Cisco UCS B200 M5 2 Socket...	FL...	org-root/org-FlexPod-SMBC/its-VM-Host...		20	20	40	13...	1	6	0	🟢 ⬆	🟢 ⬆	🟢 ⬆	N/A
Server 4	🔴 ⬇	U...	Cisco UCS B200 M4	FL...			28	28	56	26...	1	0	0	🟢 ⬆	🟢 ⬆	🔴 ⬇	N/A
Server 5	🔴 ⬇	U...	Cisco UCS B200 M6 2 Socket...	FC...			48	48	96	26...	1	0	0	🟢 ⬆	🟢 ⬆	🔴 ⬇	N/A
Server 6	🟢 ⬆	U...	Cisco UCS B200 M6 2 Socket...	FC...	org-root/org-FlexPod-SMBC/its-VM-Host...		48	48	96	26...	1	6	0	🟢 ⬆	🟢 ⬆	🟢 ⬆	N/A

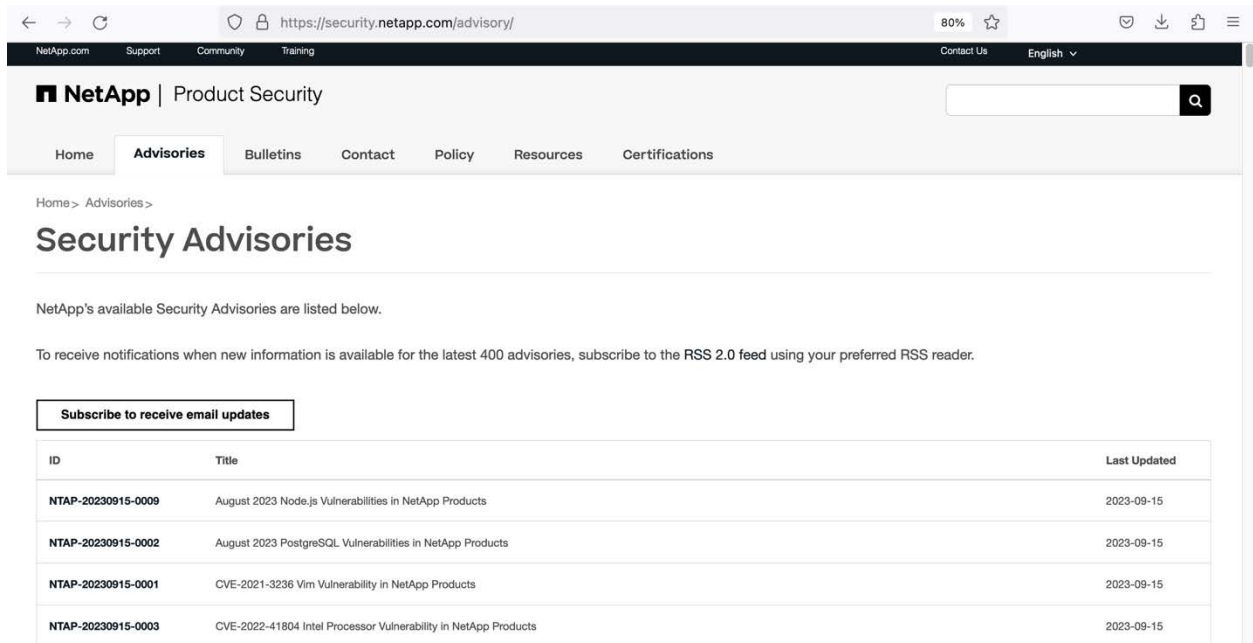
As it turned out, after this M6 server was added into the chassis recently, it had not gone through a firmware upgrade process yet for it to pick up the 4.2(3d) firmware bundle. To address this issue, we invoked the Install Server Firmware action which is available under the Firmware Auto Install tab in the Equipment view to upgrade the server firmware.

Note: For servers which have associated service profiles, you can also initiate the firmware upgrade process from Servers view within Intersight.

Note: Please refer to the FlexPod CVDs in the reference section and Intersight Help Center for more information on using Intersight for FlexPod management and additional Intersight features and functionalities.

NetApp security advisories

NetApp Security Advisories are available on NetApp security information site, <https://security.netapp.com>. On the Advisories page, <https://security.netapp.com/advisory>, you can review a list of vulnerability announcements and remediation instructions published by the NetApp Product Security Incident Response Team (PSIRT). You can click into the vulnerability ID to get detailed information on the vulnerability and remediation. You can also click on the Subscribe to receive email updates button to sign up for email notifications.



The screenshot displays the NetApp Product Security Advisories page. The header includes the NetApp logo and navigation links. The main content area is titled 'Security Advisories' and contains a list of advisories. A button labeled 'Subscribe to receive email updates' is positioned above the table. The table lists four advisories, each with an ID, a title, and a last updated date.

ID	Title	Last Updated
NTAP-20230915-0009	August 2023 Node.js Vulnerabilities in NetApp Products	2023-09-15
NTAP-20230915-0002	August 2023 PostgreSQL Vulnerabilities in NetApp Products	2023-09-15
NTAP-20230915-0001	CVE-2021-3236 Vim Vulnerability in NetApp Products	2023-09-15
NTAP-20230915-0003	CVE-2022-41804 Intel Processor Vulnerability in NetApp Products	2023-09-15

In the following example, the Node.js vulnerability (NTAP-20230915-0009) in NetApp products is documented. The information includes summary and impact of the vulnerability, the vulnerability scoring details, the affected products, software versions and fixes, workarounds, and where to obtain the software fixes.

← → ↻ <https://security.netapp.com/advisory/ntap-20230915-0009/> 80% ☆

NetApp.com Support Community Training Contact Us English

NetApp | Product Security

Home **Advisories** Bulletins Contact Policy Resources Certifications

Home > August 2023 Node.js Vulnerabilities in NetApp Products > August 2023 Node.js Vulnerabilities in NetApp Products >

August 2023 Node.js Vulnerabilities in NetApp Products

NetApp will continue to update this advisory as additional information becomes available.
This advisory should be considered the single source of current, up-to-date, authorized and accurate information from NetApp regarding Full Support products and versions.

Subscribe to receive email updates

Advisory ID: NTA-20230915-0009 Version: 1.0 Last updated: 09/15/2023 Status: Interim CVEs: CVE-2023-32002, CVE-2023-32003, CVE-2023-32004, CVE-2023-32006

Overview Affected Products Remediation Revision History

Summary
Multiple NetApp products incorporate Node.js. Node.js versions 16.0.0 prior to 16.20.1, 18.0.0 prior to 18.17.0, and 20.0.0 prior to 20.5.0 are susceptible to vulnerabilities which when successfully exploited could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS).

Impact
Successful exploitation of these vulnerabilities could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS).

Vulnerability Scoring Details

CVE	Score	Vector
CVE-2023-32002	9.8 (CRITICAL)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2023-32003	5.3 (MEDIUM)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
CVE-2023-32004	8.8 (HIGH)	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

In addition to providing the product security advisories, the NetApp security web site, <https://security.netapp.com>, is where customers can learn NetApp security policies, certifications, and find resources to help them maintain the confidentiality, integrity, and availability of their data.

VMware security advisories

VMware Security Advisories are available on VMware security advisories information site, which documents remediations for the reported VMware product security vulnerabilities. You can search for security advisories for a particular VMware product and specify a severity level, All / Critical / Important / Moderate / Low, for your search. You can also sign up to receive the latest security advisories and updates on the web site, <https://www.vmware.com/security/advisories.html>.

3. Heap out-of-bounds write vulnerability in EHCI controller (CVE-2022-31705)

Description

VMware ESXi, Workstation, and Fusion contain a heap out-of-bounds write vulnerability in the USB 2.0 controller (EHCI). VMware has evaluated the severity of this issue to be in the [Critical severity range](#) with a maximum CVSSv3 base score of [9.3](#).

Known Attack Vectors

A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. On ESXi, the exploitation is contained within the VMX sandbox whereas, on Workstation and Fusion, this may lead to code execution on the machine where Workstation or Fusion is installed.

Resolution

To remediate CVE-2022-31705 apply the patches listed in the 'Fixed Version' column of the 'Response Matrix' found below.

Workarounds

Workarounds for CVE-2022-31705 have been listed in the 'Workarounds' column of the 'Response Matrix' below.

Additional Documentation

None.

Acknowledgements

VMware would like to thank the organizers of GeekPwn 2022 and Yuhao Jiang for reporting this issue to us.

Notes

None.

Response Matrix:

Product	Version	Running On	CVE Identifier	CVSSv3	Severity	Fixed Version	Workarounds	Additional Documentation
ESXi	8.0	Any	CVE-2022-31705	5.9	Moderate 	ESXi80a-20842819	KB87617	None
ESXi	7.0	Any	CVE-2022-31705	5.9	Moderate 	ESXi70U3si-20841705	KB87617	None

Image validation

To secure a FlexPod solution, update software regularly to apply bug fixes and address security vulnerabilities is important part of the FlexPod best practices. To ensure image integrity of the software you install on your FlexPod solution components, download those images from the official software download sites from Cisco, NetApp, and VMware as shown below.

Cisco software download: <https://software.cisco.com/download/home>

NetApp software download: <https://mysupport.netapp.com/site/downloads>

VMware software download: <https://customerconnect.vmware.com/downloads>

After downloading the images, you can utilize the cryptographic hashes, e.g., sha-1, sha-256, or md5, that are provided for the images to confirm the integrity of the downloaded images.

To confirm the integrity of a downloaded image, use a sha-1, sha-256, and/or a md5 utility, such as sha1sum, sha256sum, and md5sum on a Linux distribution, to calculate your own hash for the downloaded image file. If the calculated hash matches the message digest provided on the official download site, you can be assured of the integrity of the downloaded image. An example of such image validation is provided in the ONTAP image validation subsection.

Cisco UCS Manager image validation

Cisco UCS Infrastructure Software Bundle contains the NX-OS software for the UCS fabric interconnect, firmware for the fabric extenders and I/O modules, UCS Manager, Chassis Management Controller, and UCSM Capability Catalog.

To download the Cisco UCS software bundle, you can search for the UCS Infrastructure and UCS Manager Software from the software download home page, select UCS Infrastructure Software Bundle type, and then pick the release that you would like to download.

For the example screenshot below, version 4.2(3d) and the bundle which supports UCS Fabric Interconnect 6454 was selected. You can then hover your mouse on top of the bundle image name to see the image details along with the MD5 and SHA512 checksums for the image.

The screenshot shows the Cisco Software Download page for UCS Infrastructure and UCS Manager Software. The page has a search bar at the top left and a list of releases on the left side. The release 4.2(3d) is selected. A 'Details' pop-up window is open, showing the following information:

- Description: The UCS Infrastructure Software Bundle contains: - NX-OS software for the UCS 6454 Fabric Interconnects - Firmware for the fabric extenders and I/O modules - UCS Manager - Chassis Management Controller - UCSM Capability Catalog.
- Release: 4.2(3d)
- Release Date: 21-Mar-2023
- FileName: ucs-6400-k9-bundle-infra.4.2.3d.A.bin
- Size: 2445.06 MB (2563826930 bytes)
- MD5 Checksum: fe6fa6515fadf1eb88e288c2d6a6593c
- SHA512 Checksum: facdccb0e7675c140d64434578385410 ...

The pop-up also includes links for 'Release Note for 4.2(3d)' and 'Advisories'. The background shows a table of releases with columns for Release Date and Size.

Release Date	Size
21-Mar-2023	1332.68 MB
21-Mar-2023	2445.06 MB

Cisco Nexus image validation

For Cisco Nexus NX-OS images, you can search for the NX-OS software, and then narrow down the search by selecting Switches > Data Center Switches > Nexus 9000 Series Switches, and then pick the switch model you are using and the firmware version you would like to download.

In the example screenshot below, Nexus 9336C-FX2 switch, and NX-OS software type were selected along with the 10.2(5)(M) firmware version. Once you hover your mouse on top of the Cisco Nexus 9000/3000 Standalone Switch location, the Details for the firmware information pops up. You can use the copy icon to the right of the MD5 and SHA512 checksums to copy those checksums to validate your downloaded image.

Software Download

Downloads Home / IOS and NX-OS Software / NX-OS / NX-OS Software / Switches / Data Center Switches / Nexus 9000 Series Switches / Nexus 9336C-FX2 Switch / NX-OS System Software- 10.2(5)(M)

Search...

Expand All Collapse All

3

2

10.2(6)(M)

10.2(5)(M)

10.2(4)(M)

10.2(3)(F)

10.2(2)(F)

Details

Description : Cisco Nexus 9000/3000 Standalone Switch

Release : 10.2(5)

Release Date : 07-Mar-2023

FileName : nxos64-cs.10.2.5.M.bin

Min Memory : DRAM 0 Flash 0

Size : 1853.35 MB (1943380992 bytes)

MD5 Checksum : 2f60a186cb9c2d55c90086302e51f655

SHA512 Checksum : db7805661392abc54192e3537ad6070c ...

Release Notes for 10.2(5) N3K Release Notes for 10.2(5) N9K Advisories

Related Links and Documentation

Release Notes for 10.2(5) N9K

Release Notes for 10.2(5) N3K

Release Date	Size
07-Mar-2023	62.54 MB
07-Mar-2023	1853.35 MB

NetApp image validation

For NetApp ONTAP software download, there are two different images, one with NetApp Volume Encryption included and the other without it. Be sure to review the Restrictions on Encryption Technology information on the page and select the correct one for your situation.

← → ↺ ↻

https://mysupport.netapp.com/site/products/all/details/ontap9/downloads-tab/download/62286/9.13.1P2/downloads

Centos Wiki Documentation Forums

Products > All Products > ONTAP 9 (Downloads) > 9.13.1P2

ONTAP 9 9.13.1P2

Date Posted : 08-Sep-2023

Restrictions on Encryption Technology

NetApp Volume Encryption (available with ONTAP 9.1 and later releases) provides for data-at-rest encryption that requires authorizations, permits, or licenses to import, export, re-export or use this software in certain countries (the "Restricted Countries").

By way of example, a state license for importation of encryption equipment is required to import ONTAP 9 with NetApp Volume Encryption into China and Member States of Eurasian Economic Union: Russia, Belarus, Kazakhstan, Armenia and Kyrgyzstan. Moreover, in certain cases, an end-user customer must have a valid state encryption license to use this software.

If you are still unsure which ONTAP image file to download and save, review [this article](#) for more information before continuing to download and install this version of ONTAP.

Download & Save

Please download and save the software image to an HTTP server that is accessible to your system.

If you are upgrading to ONTAP 9.13.1P2, and you are in "Non-restricted Countries", please download the image with NetApp Volume Encryption.

DOWNLOAD ONTAP 9.13.1P2 WITH NETAPP VOLUME ENCRYPTION FOR FAS [2.69 GB]

View and download checksums

Download .md5 Value: 6d19a967cd0a35741e3008caa9a646b0

Download .sha256 Value: c2798787e89226e5dec2dfc197cf050e9a9fa38f0a5129a0182de7835e65d9f

If you are unsure whether your company complied with all applicable legal requirements on encryption technology, download the image without NetApp Volume Encryption.

DOWNLOAD ONTAP 9.13.1P2 WITHOUT NETAPP VOLUME ENCRYPTION FOR FAS [2.69 GB]

View and download checksums

Download .md5 Value: 892cd0eba419fc117ee9c459c568ee

Download .sha256 Value: 6bd6087bd0369a02100f8a0842e1bae2a9459ead765609e1102de91d1fad79045

Please also note that you can click on View and download checksums link to view and download the md5 and sha256 checksums to validate the downloaded image. An example of comparing the ONTAP software image md5 and sha256 checksums against the downloaded checksums using a Linux system is shown below.

```
$ md5sum 9131P2_q_image.tgz
6d19a967cd0a35741e3008caa9a646b0 9131P2_q_image.tgz

$ cat 9131P2_q_image.tgz.md5
6d19a967cd0a35741e3008caa9a646b0 9131P2_q_image.tgz

$ sha256sum 9131P2_q_image.tgz
c2798787e89226e5dec2dfc197cff050e9a9fa38f0a5129a0182de7835e65d9f 9131P2_q_image.tgz

$ cat 9131P2_q_image.tgz.sha256
c2798787e89226e5dec2dfc197cff050e9a9fa38f0a5129a0182de7835e65d9f 9131P2_q_image.tgz
```

VMware image validation

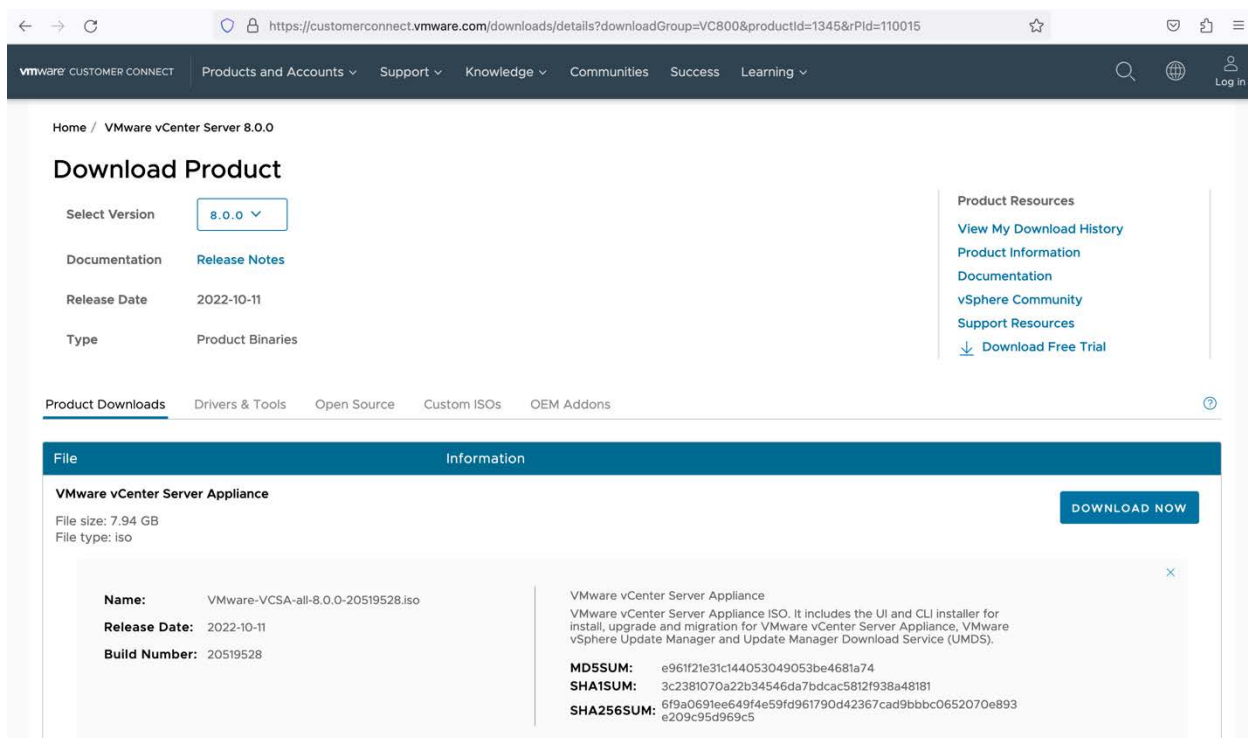
For the VMware ESXi images, be sure to utilize the Cisco Custom Images for the ESXi versions to simplify the installation as they are customized by Cisco to include the needed drivers and firmware for the UCS environment. When you click on the Read More link, additional information for the image is provided, including the various hashes you can use to validate your downloaded images.

Name:	VMware-ESXi-8.0-20513097-Custom-Cisco-4.2.3-b.iso
Release Date:	2023-02-28
Build Number:	20513097

Component--Version
CIS-ucs-tool-esxi--1.2.4-14
Cisco-nenic--1.0.45.0-IOEM.700.1.0.15843807
Cisco-nenic-ens--1.0.6.0-IOEM.700.1.0.15843807
Cisco-nfnic--5.0.0.37-IOEM.700.1.0.15843807
Intel-i40en--2.2.7.0-IOEM.700.1.0.15843807
Intel-igbn--1.9.1.0-IOEM.700.1.0.15843807
Intel-ixgbe--1.12.3.0-IOEM.700.1.0.15843807
MRVL-E3-Ethernet-iSCSI-FCoE--3.0.182.0-IOEM.700.1.0.15843807
MRVL-E4-CNA-Driver-Bundle--5.0.305.0-IOEM.700.1.0.15843807

MD5SUM:	eble8f7912750c70b90049d8ab355667
SHA1SUM:	86f5af463dfb70ad13ba6f45a04fe44059d82e49
SHA256SUM:	a9f9f0c2368ff603c7d7f1434a5d80954b3e7ee479deca6d6cdf e7a68c32e535

For VMware vCenter Server Appliance, there is no customization available. After you select the desired version to download, you can click the Read More link to see additional image details and the various checksums as shown below that are available for image validation.



Conclusion

FlexPod solutions provide reliable, flexible, and scalable infrastructure foundations for your enterprise workloads. While FlexPod is secure by design, administrators need to be aware of the potential security threats and the available tools and technologies to help harden the security of a FlexPod deployment.

In this report, we reviewed various aspects of a FlexPod solution infrastructure and highlighted some of the critical tools and technologies to help secure a FlexPod solution. For example, you can utilize various login methods and implement role-based access control. You should synchronize time on the components for proper solution operation and ease of troubleshooting and issue tracking. You should configure login banners, limit login sessions, set session timeouts, configure remote logging, and plan for scheduled configuration backups.

As a layered approach to security, you can implement network and traffic segmentation, restrict network access by using access list, and allow NFS clients access to data by correctly applying export policies. You can also configure the FlexPod components to run in FIPS 140 compliant mode but will need to observe some of the corresponding limitations and update your configurations accordingly to be compliant.

You should configure UEFI secure boot for your ESXi hosts to take advantage of the UCS server's TPM modules and boot from SAN for ease of server replacement. However, you will need to be aware of the potential security violation when you try to move a service profile for hardware replacement or upgrade and save off encryption recovery information after initial configuration to recover from the security violation scenario.

You will want to subscribe to the NetApp, Cisco, and VMware security advisories that are relevant to your FlexPod solution components, review those advisories carefully and take actions to upgrade or apply workarounds to mitigate those vulnerabilities. You can utilize Cisco Intersight to get Cisco security advisories that are specific to your environment and follow the information to quickly remediate issues.

In summary, securing your FlexPod solution is not a one-and-done effort. It is recommended that you review this report and other available security references carefully and harden your FlexPod solution security from Cisco UCS, Cisco Nexus, NetApp storage, and VMware perspectives after initial solution deployment. It is also a FlexPod best practice to be vigilantly monitoring your FlexPod solution configurations, filtering logs for potential security issues, reviewing security advisories, and performing software and firmware updates to mitigate known issues, to address and minimize security vulnerabilities, and to ensure the continuous and reliable operations of your business solutions built on FlexPod.

Appendix A: UEFI secure boot service profile move

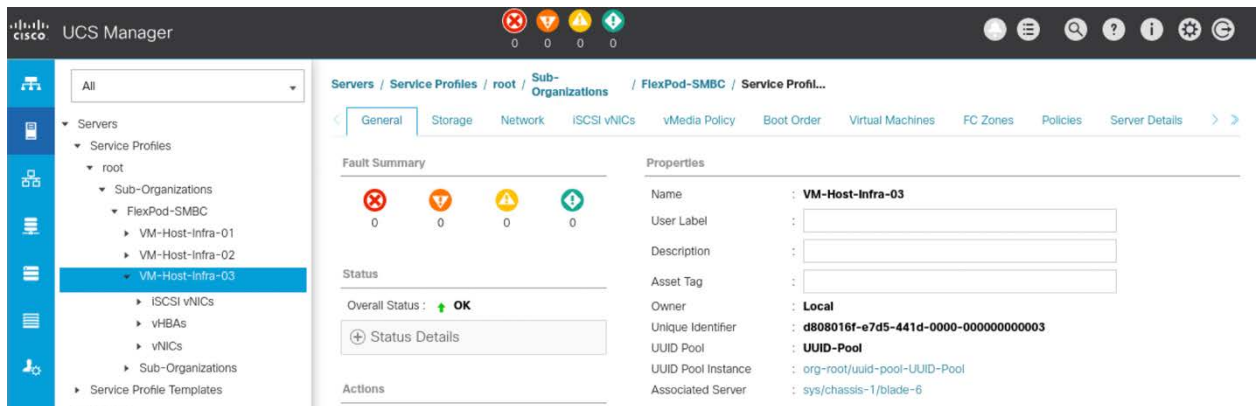
Cisco UCS supports stateless compute where a service profile can be moved from one physical server to another seamlessly. Hosts in a FlexPod solution are typically configured to boot from SAN, which makes moving a service profile simple as the same service profile can utilize the same LUN to boot on a new server.

For UEFI secure boot configuration with a TPM 2.0 module, an additional process of updating ESXi boot configuration is needed due to booting with a different server and TPM module. The following highlights the steps of moving a service profile to a different underlying physical server when using the UEFI secure boot configuration.

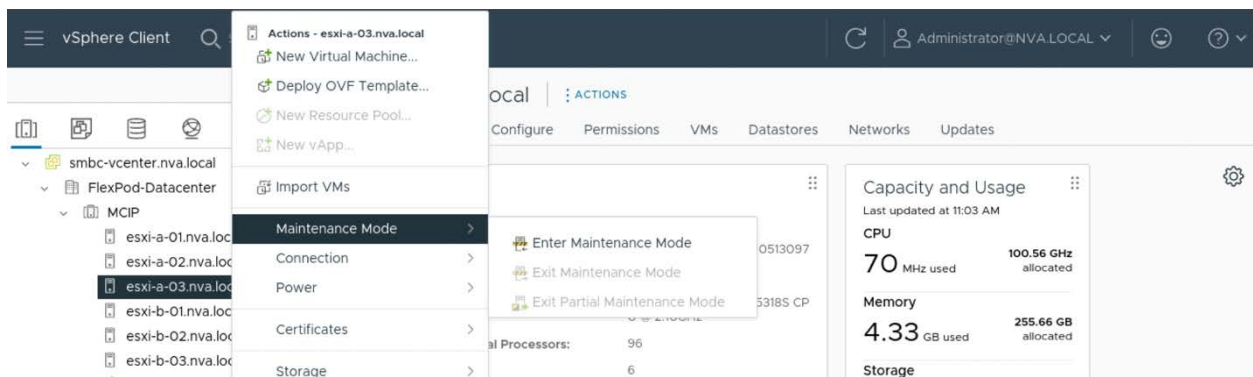
Prepare for service profile move

In this example, we are assuming that the reason behind a service profile move is to replace the underlying physical server and the existing server is still in working condition. In this case, we can put the host into maintenance mode first to migrate workloads off the host before shutting it down.

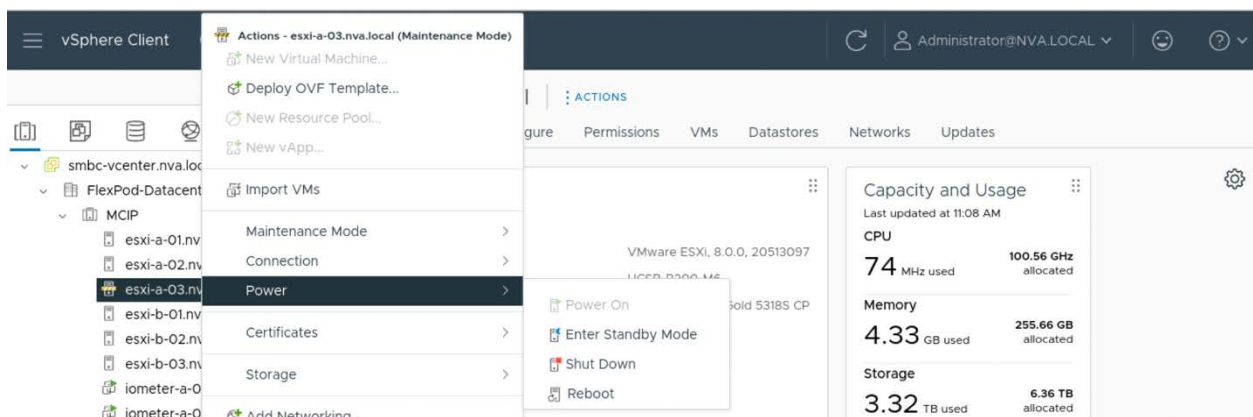
Examine the UCS Manager service profile information to identify the physical server to be replaced. Here we are replacing the server `/sys/chassis-1/blade-6` which is associated with the VM-Host-Infra-03 service profile.



Log in to vCenter Server, right-click on the server in the Inventory, select Maintenance Mode from the menu, select Enter maintenance Mode, and click Ok on the Enter Maintenance Mode dialog.



After the workload had been migrated off the server and the server had been put into Maintenance mode, right-click on the server in the Inventory, select Power, select Shut Down, provide a reason in the Shut Down Host dialog, and then click Ok to shut down the server.

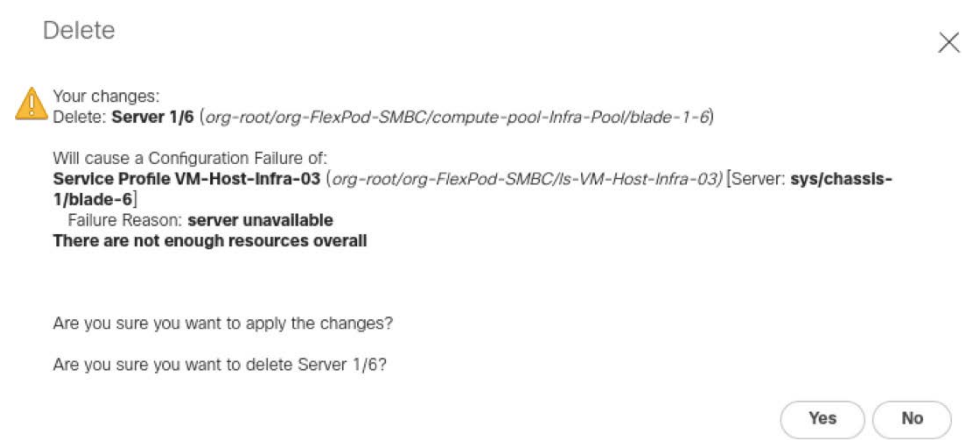
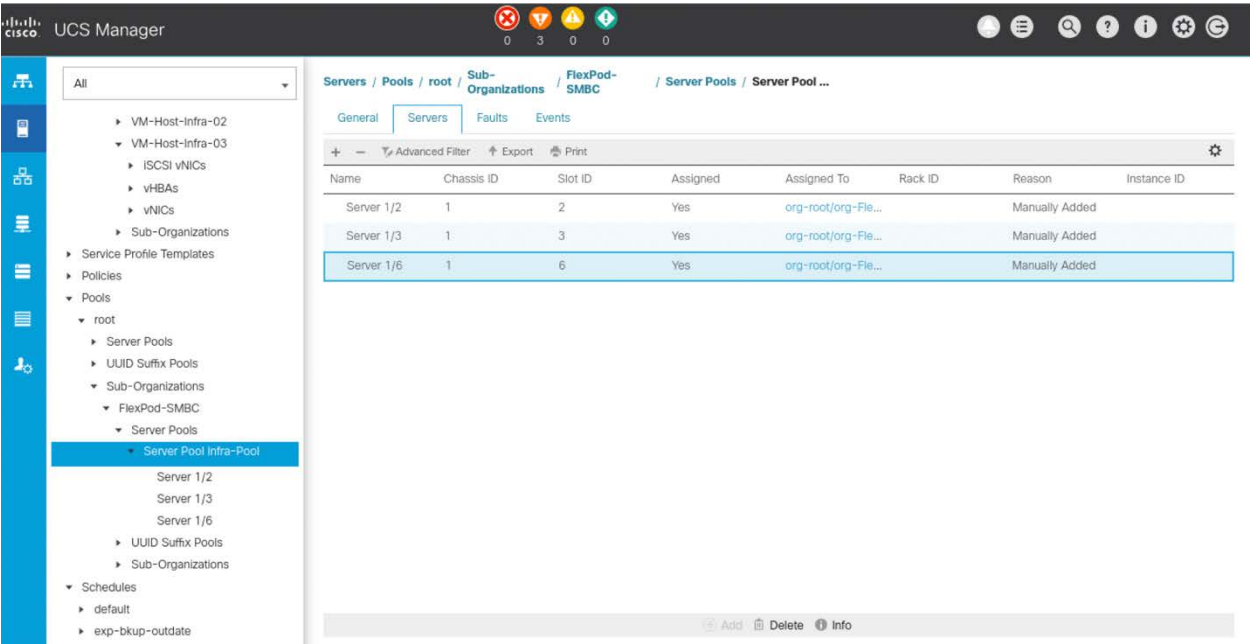


In the case of a failed server hardware, it is not possible to put the host into maintenance mode. Also, the workload should have already been migrated to the remaining hosts by the VMware HA feature configured on the FlexPod solution.

Update server pool

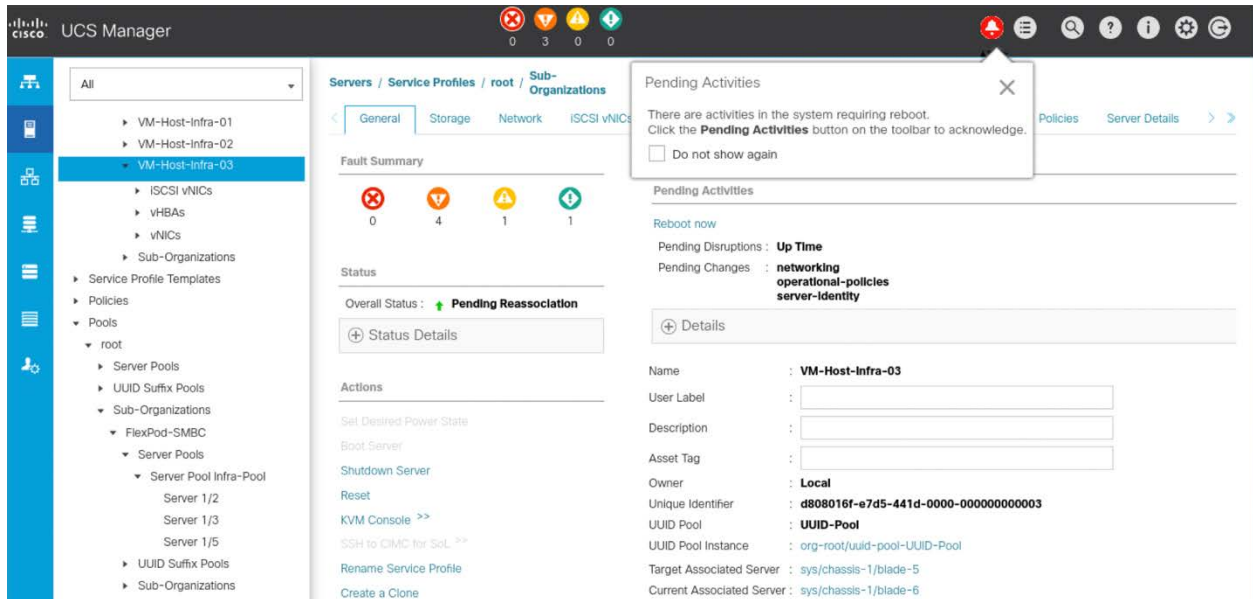
After confirming that the server is in the Power Off status in UCS Manager, we are ready to update the server pool to remove the old server and add the new server. For this example, we are removing Server 1/6 and adding Server 1/5.

Log in to UCS Manager, select Servers, expand Pools and Sub-Organizations to locate the server pool, select the server under the Servers tab, click Delete, and then click Yes to confirm the server deletion.



To add the new server, go to the General tab for the server pool, click the Add Servers action. In the Add Servers to Server Pool dialog, select the server to add on Servers list, click the >> arrow to move it into the server pool, click Ok, and click Ok again on the success message.

After the new server is added to the pool, the service profile status changed to Pending Reassociation and there is a Pending Activity for rebooting the server.



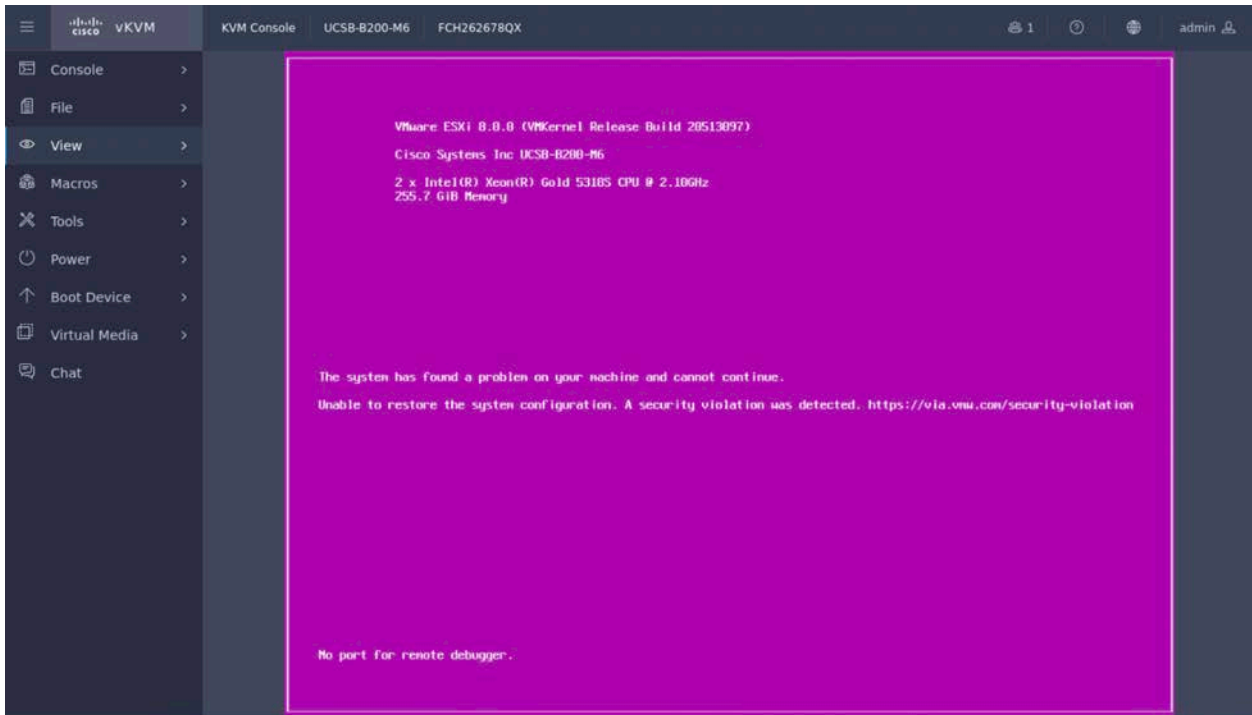
Open the Pending Activities dialog, check the Reboot Now box, click Apply, click Ok on the success message, and click Ok again to close the Pending Activities dialog. The service profile will go through configuration for the change. Afterwards, the status becomes Ok again and the server is rebooted.

Resolve service profile boot issue

When a service profile is moved from one physical server to another one with the following conditions, the ESXi host runs into purple screen of death (PSOD) and the ESXi host will fail to boot:

- TPM present in the node (Cisco UCS M5 family servers or above)
- Host installed with ESXi 7.0 U2 or above
- UEFI secure boot mode is in effect

The PSOD information is available on the server's console, which can be accessed by clicking the KVM Console link in the General tab of the service profile.

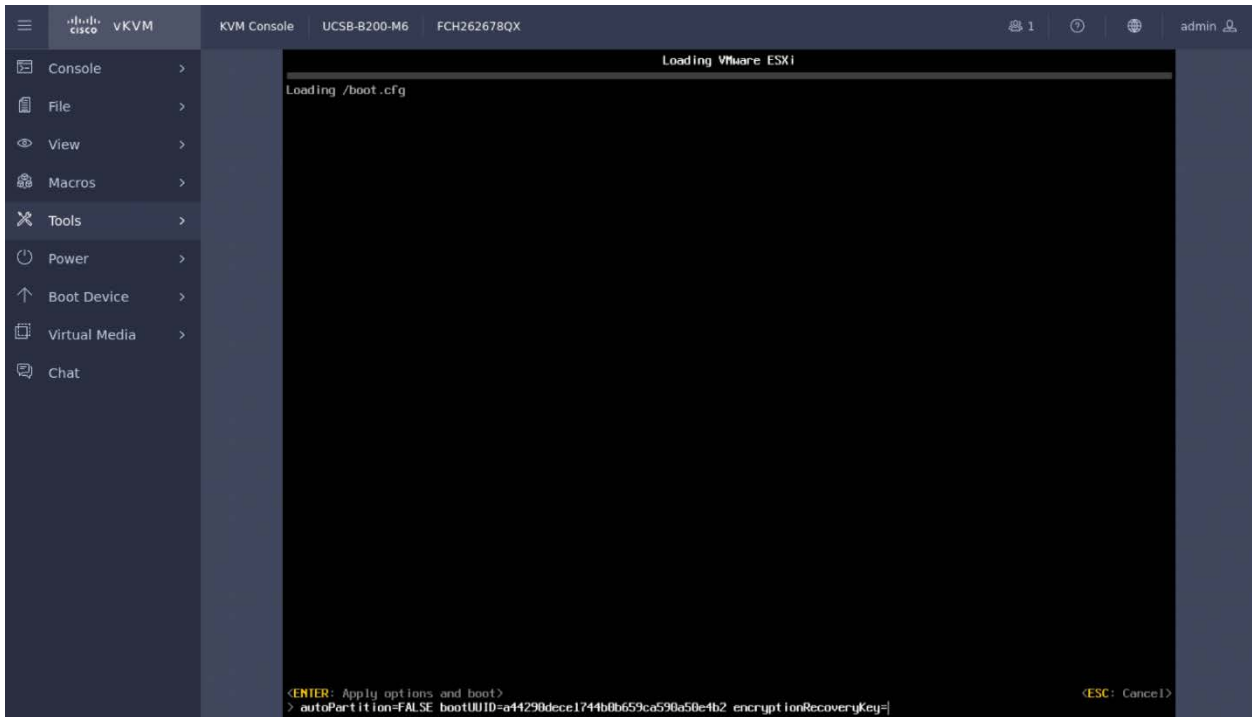


The following error message is seen on the PSOD screen.

```
The system has found a problem on your machine and cannot continue.  
Unable to restore system configuration. A security violation was detected.  
https://via.vmw.com/security-violation.
```

We will need to interrupt the server boot process to enter the encryption recovery information for the server to boot properly.

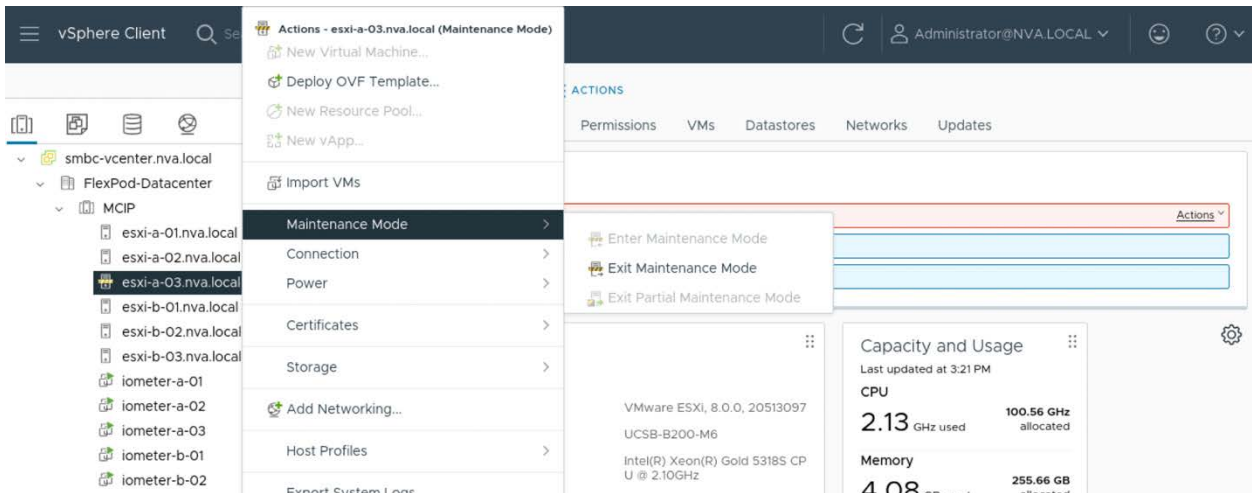
Select Power on the vKVM menu, select Reset System, click Confirm for the action, stop the ESXi boot sequence by pressing Shift + O when you see the ESXi boot screen, add the recovery key using following the boot option: encryptionRecoveryKey=<recovery_key>, and press Enter to continue the boot process.



After the ESXi host is booted, login as root user, and issue the following command to persist the encryption recovery key boot option for future boot to succeed without needing to provide it again.

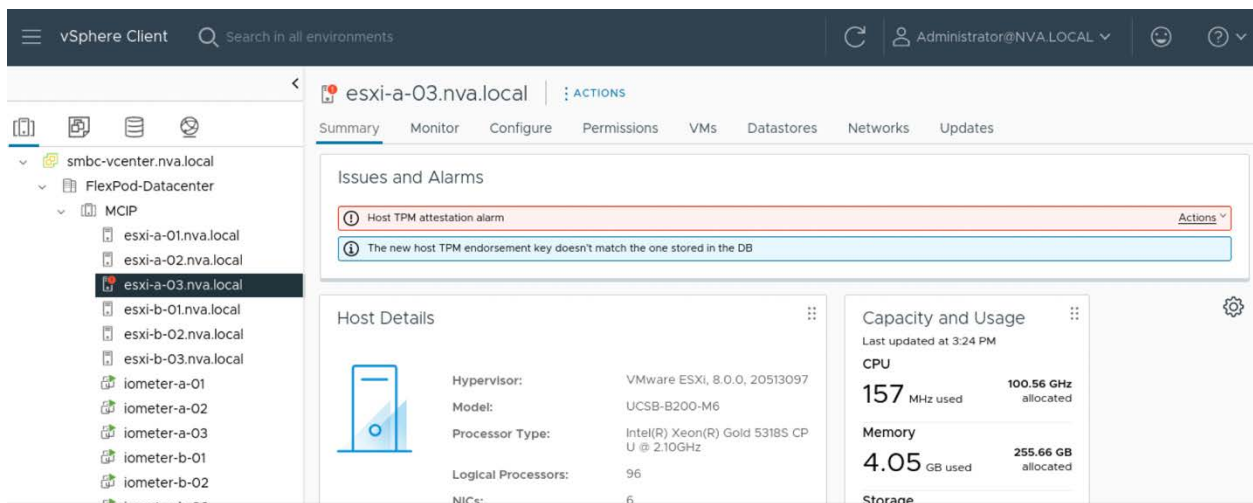
```
/sbin/auto-backup.sh
```

Log into vCenter Server, right-click on the server in the Inventory, select Maintenance Mode from the menu, select Exit maintenance Mode.



vCenter Server reports the following for the host.

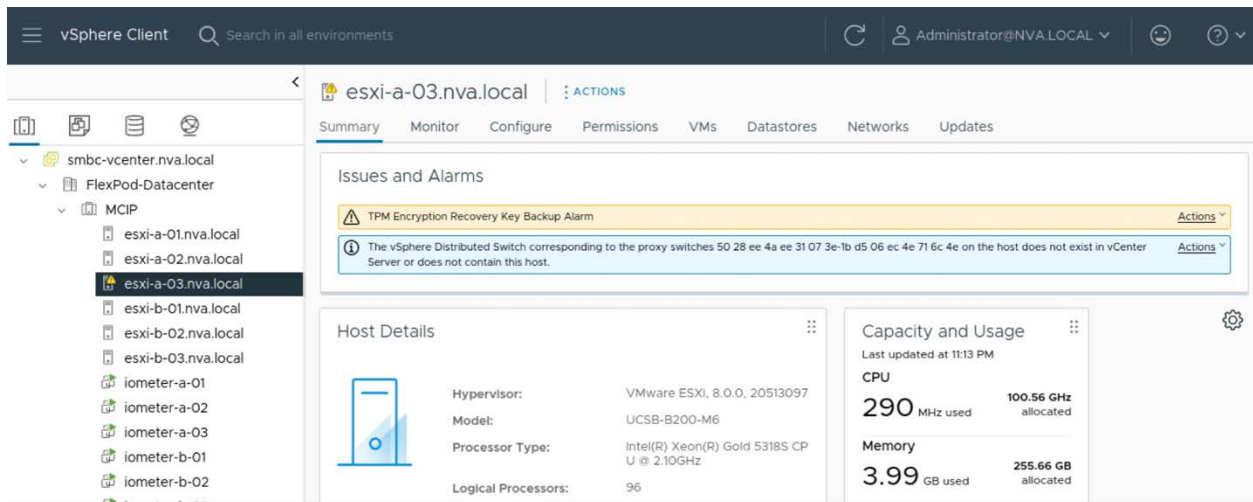
- Host TPM attestation alarm
- The new host TPM endorsement key doesn't match the one stored in the DB.



Resolve the vCenter Server reported TPM issues

To resolve the two TPM alarms shown above, put the host in Maintenance Mode, and shut it down. Once the host is disconnected from the vCenter Server, delete the host from inventory. Then, boot the host back up and add the host back into the vCenter when the host is back up.

After the host is added back into the vCenter Sever, bring it out of Maintenance Mode, then follow steps below to resolve the new encryption backup alarm, and vCenter distributed switch configuration issues.

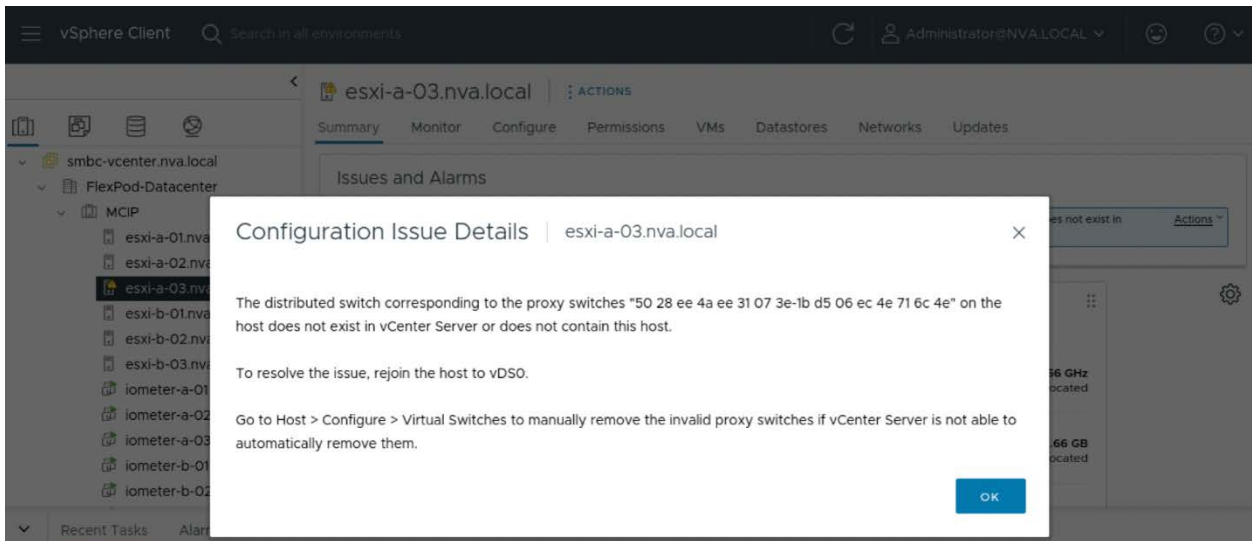


To back up the recovery key information, log into the ESXi host as the root user, list the encryption recovery information, and securely save the Recovery ID and Key information for the ESXi host.

```
[root@esxi-a-03:~] esxcli system settings encryption recovery list
Recovery ID                                     Key
-----
{F7CFD208-E7C7-4D50-8AA9-A32E2064994B} 331342-134993-057950-232411-709944-082109-239663-322153-
288450-105147-192004-074723-523744-409928-597006-546946
```

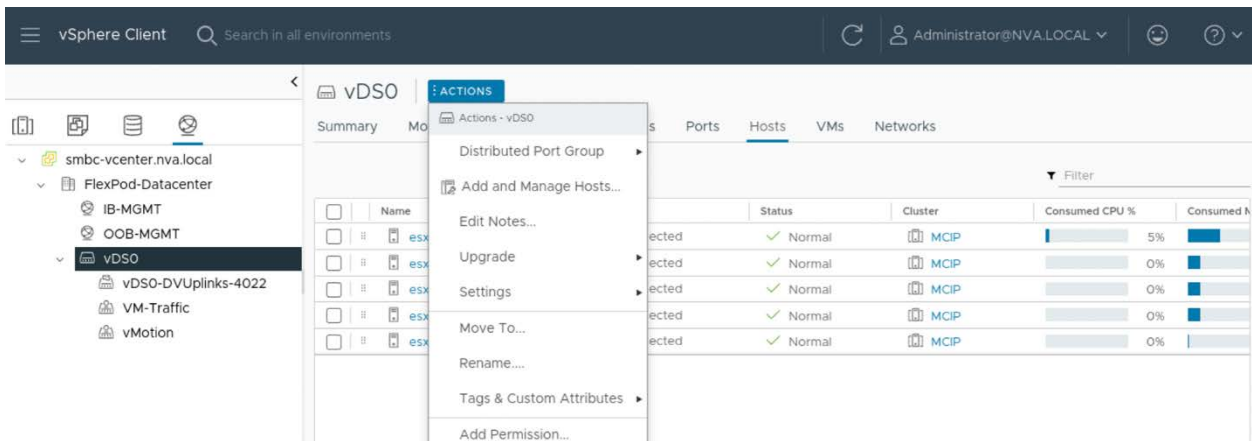
You can use the Reset to Green under Actions drop-down list to acknowledge the alarm after securely backing up the encryption recovery information for future recovery purposes.

Select Show Details under Actions drop-down list to see the vSphere Distributed Switch configuration issue and follow the information in the Configuration Issue Details below to rejoin the host to vDS0.

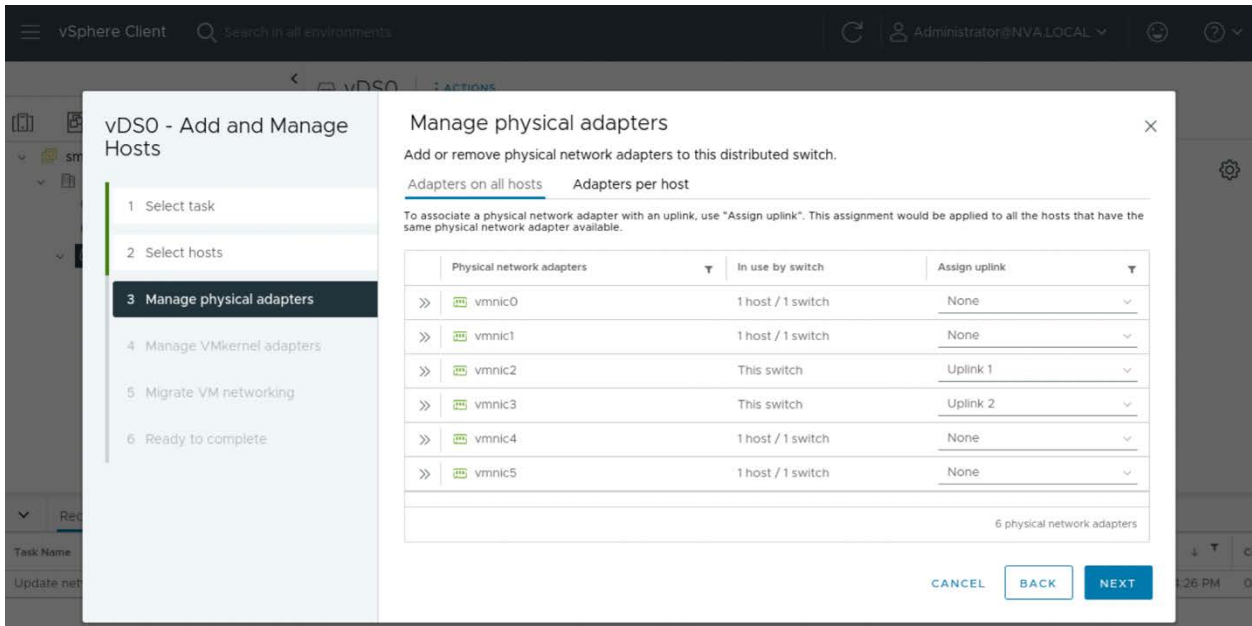


In vCenter Server, navigate to Networking tab and select the vDS0, launch the Add and Manage Hosts wizard from the ACTIONS menu.

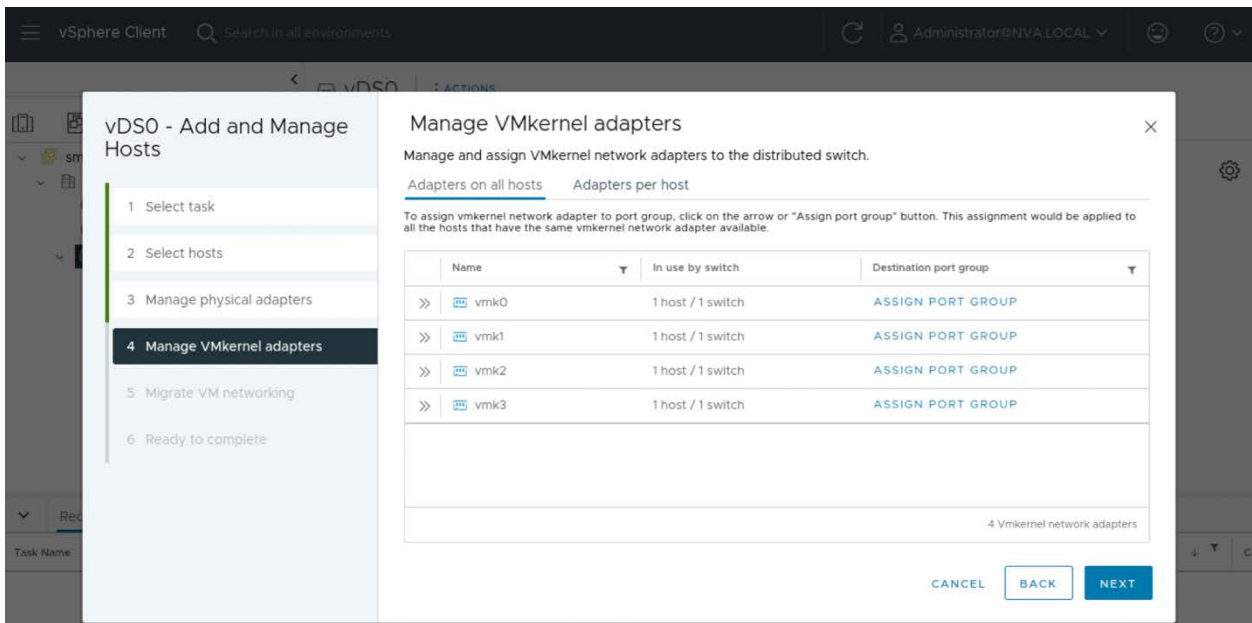
In the vDS - Add and Manage Hosts dialog, select the Add hosts task, click Next, check the box for the host to be added, click Next.



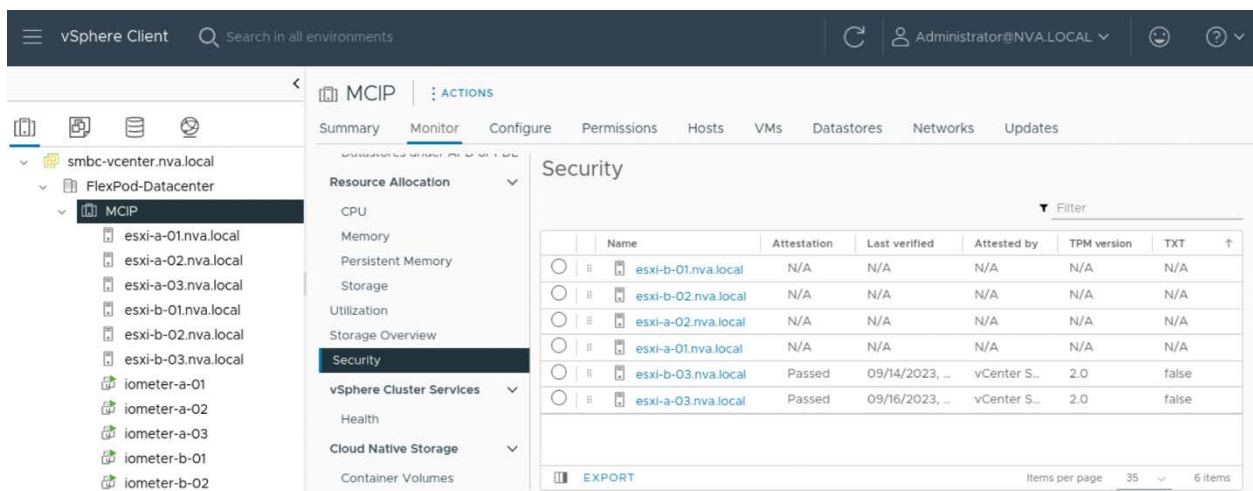
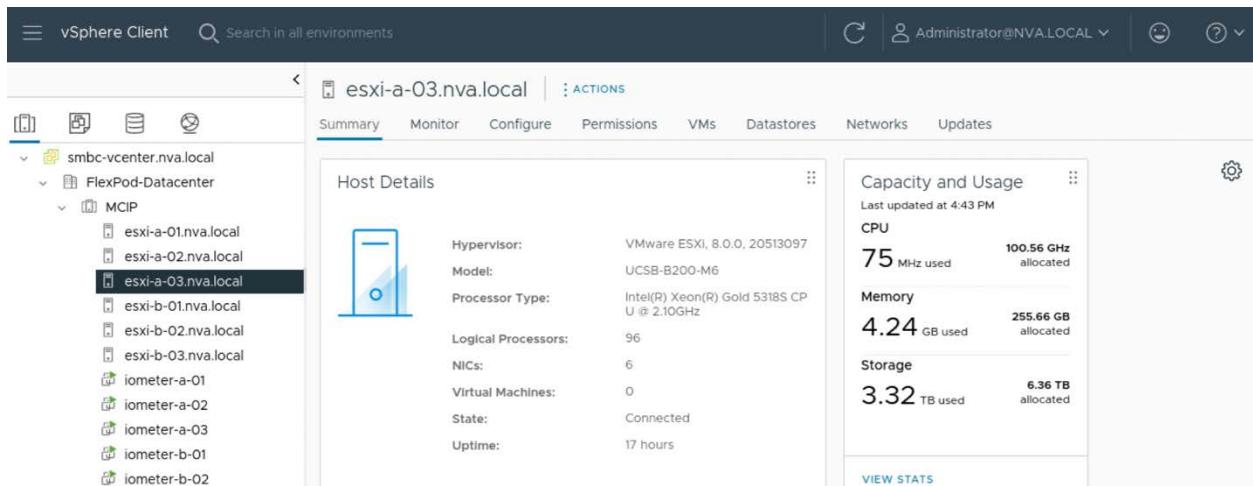
Select the appropriate physical adapters and assign the uplinks, and click Next.



Click on the arrow or Assign Port Group button to assign vmkernel adapters to port groups, click Next, migrate virtual machines to the vDS if needed, click Next, review settings, and then click Finish.



After the host rejoined the vDS0, the distributed switch alarm went away. Also, the vCenter Server Security Monitor status showed TPM attestation as Passed again.



Appendix B: ONTAP multi-admin verification example

ONTAP multi-admin verification (MAV) allows certain protected operations, such as deleting volumes or Snapshot copies, to be executed only after approvals from designated administrators. The additional verification prevents inexperienced, compromised, or malicious administrators from making undesirable changes or deleting data.

MAV is not enabled by default and requires certain configurations to be in place. When MAV is enabled, the completion of every protected operation requires approval before the operation can be completed.

Configuring MAV consists of:

- Creating one or more administrator approval groups.
- Enabling MAV functionality.
- Adding or modifying rules.

After initial configuration, these elements can be modified only by administrators in a MAV approval group (MAV administrators).

When MAV is enabled, the completion of every protected operation requires three steps:

- When a user initiates the operation, a request is generated.

- Before it can be successfully executed, at least one MAV administrator must approve the request.
- Upon approval, the user can retry the operation to complete it.

The following sections highlight the necessary steps to implement multi-admin verification. In the example below, we will create two additional administrators as MAV administrators and only require one approval for protected commands. In this case, either MAV administrator can approve an MAV request.

Add additional administrators

To utilize MAV, the cluster must have more than one administrator, since the administrator who initiates a protected operation cannot be the approver for the operation. The following example creates two additional administrators with ssh access and password authentication for the SiteA cluster.

```
SiteA:> security login create -vserver SiteA -user-or-group mavadmin1 -application ssh -
authentication-method password -role admin

Please enter a password for user 'mavadmin1':
Please enter it again:

SiteA:> security login create -vserver SiteA -user-or-group mavadmin2 -application ssh -
authentication-method password -role admin

Please enter a password for user 'mavadmin2':
Please enter it again:
```

Create an administrator approval group

Before enabling MAV, you must create an administrator approval group containing one or more administrators to be granted approve or veto authority. The following example creates an approval group named mavapproval and the group includes the two administrators created above.

```
SiteA:> security multi-admin-verify approval-group create -name mavapproval -approvers
mavadmin1,mavadmin2
```

Note: If there is only one person in the MAV approval group, that MAV administrator cannot enter protected operations; regular administrators must enter them, and the MAV administrator can only approve.

Note: If you want MAV administrators to be able to execute protected operations, the number of MAV administrators must be one greater than the number of approvals required. For example, if two approvals are required for a protected operation, and you want MAV administrators to execute them, there must be at least three people in the MAV administrator group.

Enable multi-admin verification

MAV is not enabled by default and must be enabled explicitly. After you enabled MAV, approval by administrators in a MAV approval group is required to modify it. The follow example shows how to enable MAV and check its configurations.

```
SiteA:> security multi-admin-verify modify -approval-groups mavapproval -required-approvers 1 -
enabled true

SiteA:> security multi-admin-verify show
Is      Required  Execution Approval Approval
Enabled Approvers Expiry    Expiry    Groups
-----
true    1          1h       1h       mavapproval
```

The Approval Expiry (option `-approval-expiry`) is the period within which a MAV administrator must respond to an approval request. The Execution Expiry (option `-execution-expiry`) is the period within which the requesting administrator must complete the operation. The corresponding options

for them can be specified during enablement. The default value is one hour (1h) for both periods, the minimum supported value is one second (1s), and the maximum supported value is 14 days (14d).

Add multi-admin verification rule

You create MAV rules to designate operations requiring approval. Whenever an operation is initiated, protected operations are intercepted and a request for approval is generated. Rules can be created before enabling MAV by any administrator with appropriate RBAC capabilities, but once MAV is enabled, any modification to the rule set requires MAV approval as well.

As of ONTAP 9.13.1, you can create MAV rules for the following commands.

```
cluster peer delete
event config modify
security login create
security login delete
security login modify
system node run
system node systemshell
volume delete
volume flexcache delete
volume snaplock modify
volume snapshot autodelete modify
volume snapshot delete
volume snapshot policy add-schedule
volume snapshot policy create
volume snapshot policy delete
volume snapshot policy modify
volume snapshot policy modify-schedule
volume snapshot policy remove-schedule
volume snapshot restore
vservers peer delete
```

In addition, the following commands are protected by default when MAV is enabled, but you can modify the rules to remove protection for these commands.

```
security login password
security login unlock
set
```

However, the rules for MAV system-default commands – the `security multi-admin-verify` commands – cannot be altered.

Here is a list of the default rules after MAV is enabled.

```
SiteA::> security multi-admin-verify rule show
```

Vserver	Operation	Required Approvers	Approval Groups

SiteA	security login password	-	-
	Query: -multi-admin-approver true -different-user true		
	security login unlock	-	-
	Query: -username diag		
	security multi-admin-verify approval-group create	-	-
	security multi-admin-verify approval-group delete	-	-
	security multi-admin-verify approval-group modify	-	-
	security multi-admin-verify approval-group replace	-	-
	security multi-admin-verify modify	-	-
	security multi-admin-verify rule create	-	-
	security multi-admin-verify rule delete	-	-
	security multi-admin-verify rule modify	-	-
	set	-	-
	Query: -privilege diagnostic		

11 entries were displayed.

Initiate a protected operation

When you initiate a protected operation on a cluster enabled for MAV, ONTAP automatically intercepts the operation and asks to generate a request, which must be approved by one or more administrators in a MAV approval group. Alternatively, you can create a MAV request without the dialog.

Since we have already enabled MAV, creating a rule with the `security multi-admin-verify rule create` command requires approval. The following command was issued by using the default admin user.

```
SiteA::> security multi-admin-verify rule create -operation "volume delete"

Warning: This operation requires multi-admin verification. To create a verification request use
"security multi-admin-verify request create".
      Would you like to create a request for this operation? {y|n}: y

Error: command failed: The security multi-admin-verify request (index 1) is auto-generated and
requires approval.
```

As the output indicated, the command failed as it requires approval. Since we answered yes to the command prompt for creating a request for the operation, an approval request was automatically generated.

Approve a protected operation

When administrators in a MAV approval group are notified of a pending operation execution request, they must respond with an approve or veto message within a fixed period (approval expiry). If enough approvals are not received within the approval expiry period, the requester must delete the request and make another.

MAV administrators can receive approval requests in email alerts (using EMS), or they can query the request queue from cluster CLI session, or if they have access to ONTAP System Manager. When they receive a request, they can take one of three actions: approve, reject (veto), or ignore (no action).

The following shows an example where the `mavadmin1` user logged into the cluster and checked for the pending approvals.

```
SiteA::> security multi-admin-verify request show-pending
```

Index	Operation	Query	State	Pending Approvers	Requestor
1	security multi-admin-verify rule create	-vserver SiteA -operation "volume delete" -auto-request-create true	pending	1	admin

The `mavadmin1` user, who is part of the approval group, can approve the request as shown in the example below by indicating approval and specifying the index of the pending approval. Afterwards, checking the pending approval queue again confirms that there are no more pending approvals.

```
SiteA::> security multi-admin-verify request approve -index 1

SiteA::> security multi-admin-verify request show-pending
There are no entries matching your query.
```

Complete a protected operation

After the pending command issued by the admin user is approved by the `mavadmin1` user, the admin user checks the state of the request and it is approved with 0 pending approvers.

```
SiteA::> security multi-admin-verify request show
```

Index	Operation	Query	State	Pending Approvers	Requestor
-------	-----------	-------	-------	----------------------	-----------

```
1 security multi-admin-verify rule create
    -vserver SiteA -operation "volume delete" -auto-request-create true
    approved 0 admin
```

When the request is approved, the requesting user can retry the operation within the execution expiry period. Here the admin user issues the rule create command again and this time it completed without errors. Afterwards, the request queue showed that the state of the command index 1 changed from approved to executed.

```
SiteA::> security multi-admin-verify rule create -operation "volume delete"

SiteA::> security multi-admin-verify request show
```

Index	Operation	Query	State	Pending Approvers	Requestor
1	security multi-admin-verify rule create	-vserver SiteA -operation "volume delete" -auto-request-create true	executed 0		admin

We can check the MAV rule show command output to confirm that the volume delete operation has indeed been added as a protected operation.

```
SiteA::> security multi-admin-verify rule show
```

Vserver	Operation	Required Approvers	Approval Groups
SiteA	security login password	-	-
	Query: -multi-admin-approver true -different-user true		
	security login unlock	-	-
	Query: -username diag		
	security multi-admin-verify approval-group create	-	-
	security multi-admin-verify approval-group delete	-	-
	security multi-admin-verify approval-group modify	-	-
	security multi-admin-verify approval-group replace	-	-
	security multi-admin-verify modify	-	-
	security multi-admin-verify rule create	-	-
	security multi-admin-verify rule delete	-	-
	security multi-admin-verify rule modify	-	-
	set	-	-
	Query: -privilege diagnostic		
	volume delete	-	-

12 entries were displayed.

Exercising the newly protected volume delete operation

Now that we have successfully added volume delete as a protected operation, we can create a new volume and then try to delete it to see that MAV is now protecting the volume delete operation.

Create a volume (admin user)

As the admin user, we created a new 10GB volume named test_mav_vol_1 on the aggr1_SiteA_03 aggregate and the volume creation job completed successfully.

```
SiteA::> vol create -vserver Infra_SiteA -aggregate aggr1_SiteA_03 -volume test_mav_vol_1 -state
online -size 10gb
[Job 5020] Job succeeded: Successful
```

Request for volume deletion (admin user)

As the admin user, we attempt to delete the newly created test_mav_vol_1 volume. The command failed because the volume delete operation requires multi-admin verification. We confirmed on the question prompt to creating a MAV request for the operation.

```
SiteA:>> vol delete -vserver Infra_SiteA -volume test_mav_vol_1
```

```
Warning: This operation requires multi-admin verification. To create a verification request use
"security multi-admin-verify request create".
```

```
Would you like to create a request for this operation? {y|n}: y
```

```
Error: command failed: The security multi-admin-verify request (index 2) is auto-generated and
requires approval.
```

We can check to confirm that there is now an outstanding MAV request, and that the operation is pending approval.

```
SiteA:>> security multi-admin-verify request show
```

Index	Operation	Query	State	Pending Approvers	Requestor
1	security multi-admin-verify rule create	-vserver SiteA -operation "volume delete" -auto-request-create true	executed 0		admin
2	volume delete	-vserver Infra_SiteA -volume test_mav_vol_1 -foreground true	pending 1		admin

```
2 entries were displayed.
```

Approve volume delete request (mavadmin1 user)

We then login as the mavadmin1 user to check and approve the pending request.

```
SiteA:>> security multi-admin-verify request show
```

Index	Operation	Query	State	Pending Approvers	Requestor
1	security multi-admin-verify rule create	-vserver SiteA -operation "volume delete" -auto-request-create true	executed 0		admin
2	volume delete	-vserver Infra_SiteA -volume test_mav_vol_1 -foreground true	pending 1		admin

```
2 entries were displayed.
```

```
SiteA:>> security multi-admin-verify request approve -index 2
```

After approving the request, we can check the request queue again to confirm the approval of the operation with 0 pending approvers.

```
SiteA:>> security multi-admin-verify request show
```

Index	Operation	Query	State	Pending Approvers	Requestor
1	security multi-admin-verify rule create	-vserver SiteA -operation "volume delete" -auto-request-create true	executed 0		admin
2	volume delete	-vserver Infra_SiteA -volume test_mav_vol_1 -foreground true	approved 0		admin

```
2 entries were displayed.
```

Complete volume delete operation (admin user)

After the request had been approved by the MAV administrator, the admin user can check the request status and complete the volume delete operation.

```
SiteA:>> security multi-admin-verify request show
```

Index	Operation	Query	State	Pending Approvers	Requestor
1	security multi-admin-verify rule create	-vserver SiteA -operation "volume delete" -auto-request-create true	executed 0		admin
2	volume delete	-vserver Infra_SiteA -volume test_mav_vol_1 -foreground true			

2 entries were displayed.

approved 0

admin

```
SiteA::> vol delete -vserver Infra_SiteA -volume test_mav_vol_1
```

Error: command failed: Volume test_mav_vol_1 in Vserver Infra_SiteA must be offline to be deleted.

The retry of the volume delete command failed because a volume must be in offline state before it can be deleted.

As a result, the admin user changed the volume state to offline, re-issued the volume delete command, and was able to successfully delete it.

```
SiteA::> vol offline -vserver Infra_SiteA -volume test_mav_vol_1
Volume "Infra_SiteA:test_mav_vol_1" is now offline.
```

```
SiteA::> vol delete -vserver Infra_SiteA -volume test_mav_vol_1
```

Info: Volume "test_mav_vol_1" in Vserver "Infra_SiteA" will be marked as deleted and placed in the volume recovery queue. The space used by the volume will be recovered only after the retention period of 12 hours has completed. To recover the space immediately, get the volume name using (privilege:advanced) "volume recovery-queue show test_mav_vol_1*" and then "volume recovery-queue purge -vserver Infra_SiteA -volume <volume_name>" command. To recover the volume use the (privilege:advanced) "volume recovery-queue recover -vserver Infra_SiteA -volume <volume_name>" command.

```
Warning: Are you sure you want to delete volume "test_mav_vol_1" in Vserver "Infra_SiteA" ?
{y|n}: y
[Job 5022] Job succeeded: Successful
```

```
SiteA::> vol show -vserver Infra_SiteA -volume test_mav_vol_1
There are no entries matching your query.
```

Note: For volume deletion, ONTAP provides the information message regarding volume recovery queue and retention period for a deleted volume. In addition, it requires a confirmation for the deletion.

Note: MAV is not intended for use with volumes or workflows that involve heavy automation because each automated protected task requires approval before the operation can be completed.

Note: For more information on MAV, please see ONTAP documentation on multi-admin verification.

Where to find additional information

To learn more about the information that is described in this document, review the following documents and/or websites:

FlexPod

- FlexPod Home Page
<https://www.flexpod.com>
- Cisco Validated Design and deployment guides for FlexPod:
<https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html>
- FlexPod Datacenter with Cisco UCSM M6, VMware vSphere 8, and NetApp ONTAP 9.12.1 Design Guide
https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_ucsm_m6_9_12_vsphere_8_design.html
- FlexPod Datacenter with End-to-End 100G, Cisco Intersight Managed Mode, VMware 7U3, and NetApp ONTAP 9.11 Design Guide

- https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_ucs_xseries_e2e_ontap_design.html
- FlexPod Datacenter with End-to-End 100G, Cisco Intersight Managed Mode, VMware 7U3, and NetApp ONTAP 9.11
https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_ucs_xseries_e2e_ontap_manual_deploy.html
- FlexPod Datacenter with End-to-End 100G, Cisco Intersight Managed Mode, using Infrastructure as Code (IaC), VMware 7U3, and NetApp ONTAP 9.11
https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_iac_e2d_deploy.html
- FlexPod Express for VMware vSphere 8.0 with Cisco UCS C-Series Standalone and NetApp AFF NVA
https://www.netapp.com/pdf.html?item=/media/88340-NVA-FlexpodExpress_C220_A250_NexusFinal.pdf
- FlexPod Express for VMware vSphere 7.0 with Cisco UCS Mini and NetApp AFF/FAS NVA Design Guide
<https://www.netapp.com/pdf.html?item=/media/22621-nva-1154-DESIGN.pdf>
- FlexPod Express for VMware vSphere 8.0 with Cisco UCS C-Series Standalone and NetApp AFF using Infrastructure as Code (IaC) NVA
<https://www.netapp.com/pdf.html?item=/media/91691-flex-pod-express-nva-ia-c.pdf>
- FlexPod Express for VMware vSphere 7.0 with Cisco UCS Mini and NetApp AFF/FAS NVA Deployment Guide
<https://www.netapp.com/pdf.html?item=/media/21938-nva-1154-DEPLOY.pdf>
- FlexPod MetroCluster IP with VXLAN Multi-Site Frontend Fabric
<https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/flexpod-metrocluster-ip-vxlan-multi-site-wp.pdf>
- TR-4920: FlexPod Datacenter with NetApp SnapMirror Business Continuity and ONTAP 9.10
<https://docs.netapp.com/us-en/flexpod/flexpod-dc/sm-bcs-introduction.html>
- TR-4892: FIPS 140-2 security-compliant FlexPod solution for healthcare
<https://docs.netapp.com/us-en/flexpod/security/flexpod-fips-introduction.html>
- TR-4961: FlexPod ransomware protection & recovery with NetApp Cloud Insights and SnapCenter
<https://www.netapp.com/media/83205-tr-4961.pdf>
- FlexPod Automation with Ansible: Accelerate your infrastructure deployment
<https://netapp.io/2022/08/09/flexpod-automation-with-ansible-accelerate-your-infrastructure-deployment/>

Cisco UCS

- Cisco Servers - Unified Computing System (UCS)
<https://www.cisco.com/c/en/us/products/servers-unified-computing/index.html>
- Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 4.2
https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/cli/config/guide/4_2/b_cisco_ucs_c-series_cli_configuration_guide_42/b_Cisco_UCS_C-Series_CLI_Configuration_Guide_41_chapter_01100.html
- Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide, Release 4.2

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/gui/config/guide/4_2/b_cisco_ucs_c-series_gui_configuration_guide_42/b_Cisco_UCS_C-series_GUI_Configuration_Guide_41_chapter_01110.html

- FIPS 140-2 Level 1 Security Policy for Cisco Secure ACS FIPS Module
<https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp948.pdf>
- Cisco UCS Manager Administration Management Guide 4.2
https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Admin-Management/4-2/b_Cisco_UCS_Admin_Mgmt_Guide_4-2/m_password_management.html
- Cisco UCS Manager System Monitoring Guide, Release 4.2
https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/System-Monitoring/4-2/b-UCSM-GUI-System-Monitoring-Guide-4-2/b_UCSM_GUI_System_Monitoring_Guide_chapter_01000.html

Cisco Nexus

- Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 10.2(x)
<https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/102x/configuration/Security/cisco-nexus-9000-nx-os-security-configuration-guide-102x.html>

Cisco Intersight

- Intersight help center
<https://intersight.com/help/appliance>

NetApp ONTAP

- ONTAP product documentation
<https://docs.netapp.com/us-en/ontap-family/>
- SnapMirror business continuity
<https://docs.netapp.com/us-en/ontap/smbc/index.html>
- TR-4878 - SnapMirror Business Continuity (SM-BC) ONTAP 9.8
<https://www.netapp.com/pdf.html?item=/media/21888-tr-4878.pdf>
- SnapMirror Synchronous disaster recovery basics
<https://docs.netapp.com/us-en/ontap/data-protection/snapmirror-synchronous-disaster-recovery-basics-concept.html>
- Asynchronous SnapMirror disaster recovery basics
<https://docs.netapp.com/us-en/ontap/data-protection/snapmirror-disaster-recovery-concept.html#data-protection-relationships>
- Data protection and disaster recovery
<https://docs.netapp.com/us-en/ontap/data-protection-disaster-recovery/index.html>
- SnapMirror configuration and best practices guide for ONTAP 9
<https://www.netapp.com/media/17229-tr4015.pdf>
- TR-4569: Security hardening guide for NetApp ONTAP
<https://www.netapp.com/media/10674-tr4569.pdf>
- TR-4572: The NetApp solution for ransomware
<https://www.netapp.com/media/7334-tr4572.pdf>
- KB: Native FPolicy File Blocking
https://kb.netapp.com/onprem/ontap/da/NAS/Native_FPolicy_File_Blocking
- ONTAP 9.13.1 EMS Reference

<https://docs.netapp.com/us-en/ontap-ems-9131/>

VMware vSphere

- vSphere Security
<https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-esxi-vcenter-801-security-guide.pdf>
- vSphere Authentication
<https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-esxi-vcenter-801-authentication-guide.pdf>
- vSphere 8 Security Configuration & Hardening Guide
<https://core.vmware.com/vmware-vsphere-8-security-configuration-guide>
- Best Practices for Running NFS with VMware vSphere
<https://core.vmware.com/resource/best-practices-running-nfs-vmware-vsphere>
- VMware vCenter Server Management Programming Guide
<https://developer.vmware.com/docs/12016>
- Monitoring Events, Alarms, and Automated Actions
<https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-monitoring-performance/GUID-9272E3B2-6A7F-427B-994C-B15FF8CADC25.html>
- VMware Security Advisories
<https://www.vmware.com/security/advisories.html>

Example security incidents

- Okta: Caesars, MGM hacked in social engineering campaign
<https://www.techtarget.com/searchSecurity/news/366552775/Okta-Caesars-MGM-hacked-in-social-engineering-campaign>
- 4 Okta customers hit by campaign that gave attackers super admin control
<https://arstechnica.com/security/2023/09/4-okta-customers-hit-by-campaign-that-gave-attackers-super-admin-control/>

Tools

- How to install syslog on RHEL 8 / CentOS 8
<https://linuxconfig.org/install-syslog-on-redhat-8>
- How to Install Secure FTP Server on CentOS 8
<https://www.centlinux.com/2020/01/how-to-install-secure-ftp-server-centos-8.html>

VMware vSphere HA and vSphere Metro Storage Cluster

- Creating and Using vSphere HA Clusters
<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.avail.doc/GUID-5432CA24-14F1-44E3-87FB-61D937831CF6.html>
- VMware vSphere Metro Storage Cluster (vMSC)
<https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-vmssc>
- VMware vSphere Metro Storage Cluster Recommended Practices
<https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-recommended-practices>
- NetApp ONTAP with NetApp SnapMirror Business Continuity (SM-BC) with VMware vSphere Metro Storage Cluster (vMSC). (83370)
<https://kb.vmware.com/s/article/83370>
- Protect tier-1 applications and databases with VMware vSphere Metro Storage Cluster and ONTAP

<https://community.netapp.com/t5/Tech-ONTAP-Blogs/Protect-tier-1-applications-and-databases-with-VMware-vSphere-Metro-Storage/ba-p/171636>

Standards and Policies

- FIPS 140-3: Security Requirements for Cryptographic Modules
<https://csrc.nist.gov/pubs/fips/140-3/final>
- FIPS 140-2: Security Requirements for Cryptographic Modules
<https://csrc.nist.gov/pubs/fips/140-2/final>
- Cryptographic Module Validation Program CMVP
<https://csrc.nist.gov/projects/cryptographic-module-validation-program>
- NetApp Federal Information Processing Standard (FIPS) Publication 140
<https://www.netapp.com/esg/trust-center/compliance/fips-140/>
- Cisco FIPS 140
- <https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html>
- Secure by Design: Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software
<https://www.cisa.gov/resources-tools/resources/secure-by-design>

Compatibility Matrix

- Cisco UCS Hardware Compatibility Matrix
<https://ucshcltool.cloudapps.cisco.com/public/>
- NetApp Interoperability Matrix Tool
<https://support.netapp.com/matrix/>
- NetApp Hardware Universe
<https://hwu.netapp.com>
- VMware Compatibility Guide
<http://www.vmware.com/resources/compatibility/search.php>

Version history

As an option, use the NetApp Table style to create a Version History table. Do not add a table number or caption.

Version	Date	Document version history
Version 1.0	November 2023	Initial release
Version 1.1	August 2025	C-series positioning update
Version 1.2	September 2025	vsadmin-volume role capabilities update

Refer to the [Interoperability Matrix Tool \(IMT\)](#) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright information

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.