Deploy Cisco Tetration Virtual Appliance on Cisco HyperFlex Systems

Author: Hui Chen

Last Updated: December 3, 2018

Note: This document contains material and data with multiple dependencies. The information may be updated as and when necessary and is subject to change without notice.

Contents

Executive summary

The Cisco® Tetration platform is designed to address data center operational and security challenges by providing comprehensive workload protection and insights across a multicloud infrastructure. It is powered by big data technologies using unsupervised machine learning, behavior analysis, and algorithmic approaches. It provides a ready-to-use solution to accurately identify applications running in the data center and their dependencies and the underlying policies that govern the different application tiers. The platform is also designed to implement a zero-trust model using whitelist policy and segmentation, monitor the behavior of the processes running on the servers, and identify software-related vulnerabilities and exposures. With this approach, the Cisco Tetration platform provides multidimensional security across virtualized and bare-metal workloads running in a multicloud environment.

The Cisco Tetration platform has three types of deployment options: Cisco Tetration Analytics™ platform (large form factor [LFF] and small form factor [SFF]), Cisco Tetration Software as a Service (SaaS), and Cisco Tetration Virtual (Tetration-V). The virtual appliance model, Cisco Tetration-V, provides the option to run the Cisco Tetration software in on-premises VMware ESXi virtualized environments. This deployment model decouples the requirements of hardware and software, giving customers the flexibility to choose independent hardware and storage devices for running the Cisco Tetration software. It is well suited for smaller deployments such as data centers that host fewer than 1000 workloads.

Cisco HyperFlex™ systems provide an all-purpose virtualized server platform, with hypervisor hosts, network connectivity, and virtual server storage across a set of Cisco HyperFlex HX-Series x86 rack-mount servers. The platform combines the converged computing and networking capabilities provided by the Cisco Unified Computing System™ (Cisco UCS®) with next-generation hyperconverged storage software to uniquely provide the computing resources, network connectivity, storage, and hypervisor platform needed to run an entire virtual environment, all contained in a single uniform system.

Cisco HyperFlex systems deliver many enterprise-class features, such as:

- A fully distributed log-structured file system that supports thin provisioning
- High performance and low latency from the flash-friendly architecture
- In-line data optimization with deduplication and compression
- Fast and space-efficient clones through metadata operations
- The flexibility to scale out computing and storage resources separately
- Data-at-rest encryption using hardware-based self-encrypting disks (SEDs)
- Non-Volatile Memory Express (NVMe)–based solid-state disk (SSD) support
- Native replication of virtual machine snapshots

The Cisco Tetration virtual appliance on the Cisco HyperFlex HX Data Platform enables a validated data center security solution with simplified deployment; ease of day-to-day management; and integrated resources for computing, networking, and high-performance storage.

Solution overview

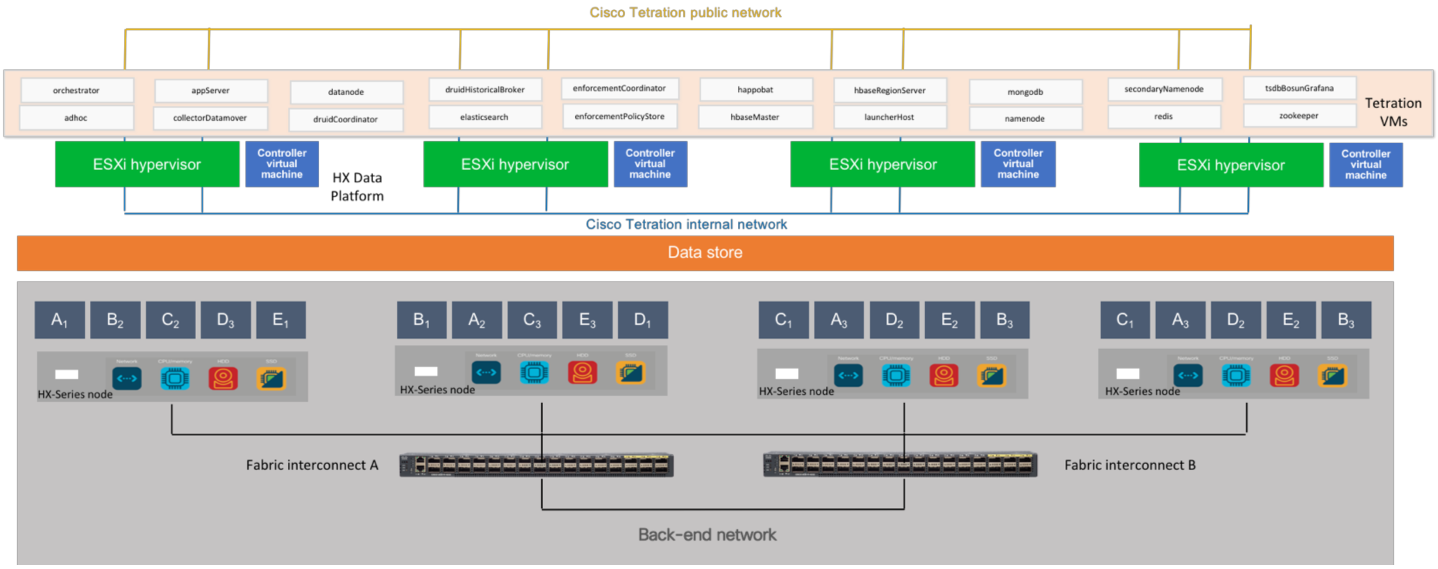
The virtual appliance deployment option of the Cisco Tetration platform lets the customer choose the underlying hardware. This choice is important because the efficiency of the infrastructure affects the efficiency of the application and the speed of data collection and processing, storage performance, and resource management.

Cisco HyperFlex systems let you unlock the full potential of hyperconvergence and adapt IT to the needs of your workloads. The systems use an end-to-end software-defined infrastructure approach that combines software-defined computing in the form of Cisco HyperFlex HX-Series nodes, software-defined storage with the powerful Cisco HX Data Platform, and software-defined networking with the Cisco UCS fabric that integrates seamlessly with Cisco Application Centric Infrastructure (Cisco ACI). These technologies together offer a single point of connectivity and management and deliver a validated and adaptable cluster with a unified pool of resources that you can quickly deploy, scale, and manage to efficiently power your applications and your business. A proven industry-leading hyperconverged platform, Cisco HyperFlex systems are an optimized choice for a Cisco Tetration-V deployment in a VMware ESXi virtual environment. By combining Cisco HyperFlex systems with Cisco Tetration data analytics software, this solution delivers an appliance-like Cisco Tetration platform with exceptional agility, quick deployment, and easy management.

This document describes how to build a Cisco Tetration virtual appliance in a dedicated Cisco HyperFlex cluster. It provides guidance about the hardware and software requirements and instructions about how to deploy Tetration-V on Cisco HyperFlex hyperconverged infrastructure.

Figure 1 provides an overview of the solution.

Figure 1. High-level solution overview



Cisco HyperFlex systems

Cisco HyperFlex systems are built on the Cisco UCS platform. They can be deployed quickly and are highly flexible and efficient, reducing risk for the customer. A main goal of the systems is simplicity of deployment and operation. They provide a hyperconverged platform that allows you to start small and grow in small increments without the need for expensive storage devices connected to computing resources through a SAN or network-attached storage (NAS).

The Cisco HyperFlex solution delivers a new generation of flexible, scalable, enterprise-class hyperconverged solutions. The solution also delivers storage efficiency features such as thin provisioning, data deduplication, and compression for greater capacity and enterprise-class performance. Additional operational efficiency is facilitated through features such as cloning and snapshots.

The complete end-to-end hyperconverged solution provides the following benefits to customers:

- **Simplicity:** The solution is designed to be deployed and managed easily and quickly through familiar tools and methods. No separate management console is required for the Cisco HyperFlex solution.
- **Centralized hardware management:** The cluster hardware is managed in a consistent manner by service profiles in Cisco UCS Manager. Cisco UCS Manager also provides a single console for solution management, including firmware management. Cisco HyperFlex HX Data Platform clusters are managed through a plug-in to VMware vCenter.
- **High availability:** Component redundancy is built in to most levels at the node. Cluster-level tolerance of node, network, and fabric interconnect failures is implemented as well.
- **Enterprise-class storage features**: Complementing the other management efficiencies are features such as thin provisioning, data deduplication, compression, cloning, and snapshots to address concerns related to overprovisioning of storage.
- **Flexibility with a “pay-as-you-grow” model:** Customers can purchase the exact amount of computing and storage they need and expand one node at a time up to the supported cluster node limit.
- **Agility to support different workloads:** Support for both hybrid and all-flash models allows customers to choose the right platform configuration for capacity-sensitive applications or performance-sensitive applications according to budget requirements.

A Cisco HyperFlex system is composed of the following components:

- One pair of Cisco UCS 6200 or 6300 Series Fabric Interconnects
- Cisco HyperFlex HX-Series HX220c or HX240c (M4 and M5) rack-mount servers
- Cisco HyperFlex HX Data Platform software
- VMware vSphere ESXi hypervisor
- VMware vCenter Server (supplied by the end user)

A Cisco HyperFlex cluster requires a minimum of three HX-Series nodes. Data is replicated across at least two of these nodes, and a third node is required for continuous operation in the event of a single-node failure. The HX-Series nodes combine the CPU and RAM resources for hosting guest virtual machines with a shared pool of the physical storage resources used by the HX Data Platform software. HX-Series hybrid nodes use a combination of solid-state disks (SSDs) for caching and hard-disk drives (HDDs) for the capacity layer. HX-Series all-flash nodes use SSD or NVMe storage for the caching layer and SSDs for the capacity layer.

Cisco HyperFlex HX-Series M5 servers are recommended for this solution.

Cisco HyperFlex HX240c M5SX Node

The Cisco HyperFlex HX240c M5SX Node (Figure 2) rack server is two rack units (2RU) high and can mount in an industry-standard 19-inch rack. This capacity-optimized hybrid model contains a minimum of six and up to twenty-three 1.8- or 1.2-TB SAS SFF HDDs that contribute to cluster storage, a 240-GB SSD housekeeping drive, a single 1.6-TB SSD caching drive installed in a rear hot-swappable slot, and a 240-GB M.2 form factor SSD that acts as the boot drive.

Figure 2. Cisco HyperFlex HX240c M5SX Node

Cisco HyperFlex HXAF240c M5SX All Flash Node

The Cisco HyperFlex HX240c M5SX All Flash Node (Figure 3) rack server is 2RU high and can mount in an industry-standard 19-inch rack. This capacity-optimized all-flash model contains a 240-GB M.2 form-factor SSD that acts as the boot drive; a 240-GB housekeeping SSD; a 375-GB Optane NVMe SSD, 1.6-TB NVMe SSD, or 400-GB SAS SSD write-log drive installed in a rear hot-swappable slot; and six to twenty-three 960-GB or 3.8-TB SATA SSD drives for storage capacity.

Figure 3. Cisco HyperFlex HX240c M5SX All Flash Node

Cisco HyperFlex HX220c M5SX Node

The Cisco HyperFlex HX220c M5SX Node (Figure 4) rack server is 1RU high and can mount in an industry-standard 19-inch rack. This small-footprint hybrid model contains a minimum of six, and up to eight 1.8- or 1.2-TB SAS HDDs that contribute to cluster storage capacity, a 240-GB SSD housekeeping drive, a 480- or 800-GB SSD caching drive, and a 240-GB M.2 form-factor SSD that acts as the boot drive.

Figure 4. Cisco HyperFlex HX220c M5SX Node

Cisco HyperFlex HX220c M5SX All Flash Node

The Cisco HyperFlex HX240c M5SX All Flash Node (Figure 5) rack server is 1RU high and can mount in an industry-standard 19-inch rack. This small-footprint all-flash model contains a 240-GB M.2 form-factor SSD that acts as the boot drive; a 240-GB housekeeping SSD; a 375-GB Optane NVMe SSD, 1.6-TB NVMe SSD, or 400-GB SAS SSD write-log drive; and six to eight 960-GB or 3.8-TB SATA SSDs for storage capacity.

Figure 5. Cisco HyperFlex HX220c M5SX All Flash Node

Cisco HyperFlex HX Data Platform software

The Cisco HyperFlex HX Data Platform is a purpose-built, high-performance, distributed file system with a wide range of enterprise-class data management services. The data platform's innovations redefine distributed storage technology, exceeding the boundaries of first-generation hyperconverged infrastructures. The data platform simplifies operations and helps ensure data availability with many enterprise-class storage features.

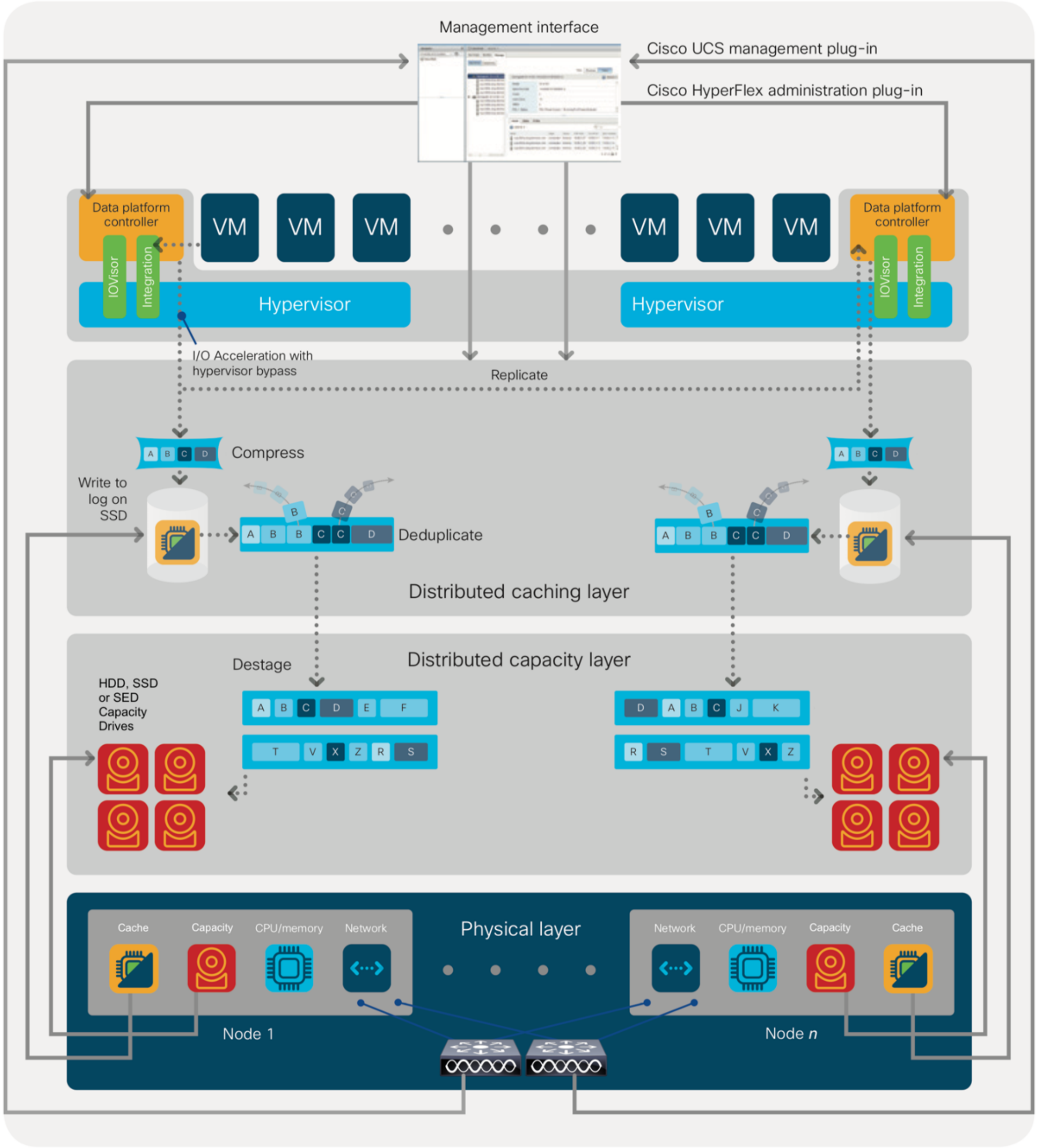
The HX Data Platform can be administered through a VMware vSphere web client plug-in or through the HTML5-based native Cisco HyperFlex Connect management tool. In addition, since HX Data Platform Release 2.6, Cisco HyperFlex systems also can be managed remotely by the Cisco Intersight™ cloud-based management platform. Through the centralized point of control for the cluster, administrators can create data stores, monitor the data platform health, and manage resource use.

An HX Data Platform controller resides on each node and implements the Cisco HyperFlex HX Distributed File System. The storage controller runs in user space within a virtual machine, intercepting and handling all I/O requests from guest virtual machines. The storage controller virtual machine uses the VMDirectPath I/O feature to provide PCI pass-through control of the physical server's SAS disk controller. This approach gives the controller virtual machine full control of the physical disk resources. The controller integrates the data platform into VMware software through three preinstalled VMware ESXi vSphere Installation Bundles (VIBs): the VMware API for Array Integration (VAAI), a customized IOvisor agent that acts as a stateless Network File System (NFS) proxy, and a customized stHypervisorSvc agent for Cisco HyperFlex data protection and virtual machine replication.

The HX Data Platform controllers handle all read and write requests from the guest virtual machines to the virtual machine disks (VMDKs) stored in the distributed data stores in the cluster. The data platform distributes the data across multiple nodes of the cluster and across multiple capacity disks in each node according to the replication-level policy selected during cluster setup. The replication-level policy is defined by the replication factor (RF) parameter. When RF = 3, a total of three copies of the blocks are written and distributed to separate locations for every I/O write committed to the storage layer; when RF = 2, a total of two copies of the blocks are written and distributed.

Figure 6 shows the movement of data in the HX Data Platform.

Figure 6. Cisco HyperFlex HX Data Platform data movement



For each write operation, the data is intercepted by the IO Visor module on the node on which the virtual machine is running, a primary node is determined for that particular operation through a hashing algorithm, and the data is then sent to the primary node. The primary node compresses the data in real time and writes the compressed data to its caching SSD, and replica copies of that compressed data are written to the caching SSD of the remote nodes in the cluster, according to the replication factor setting. Because the virtual disk contents have been divided and spread out through the hashing algorithm, the result of this method is that all write operations are spread across all nodes, avoiding problems related to data locality and helping prevent “noisy” virtual machines from consuming all the I/O capacity of a single node. The write operation will not be acknowledged until all three copies are written to the caching-layer SSDs. Written data is also cached in a write log area resident in memory in the controller virtual machine, along with the write log on the caching SSDs. This process speeds up read requests when read operations are requested on data that has recently been written.

The HX Data Platform constructs multiple write caching segments on the caching SSDs of each node in the distributed cluster. As write-cache segments become full, and based on policies accounting for I/O load and access patterns, those write-cache segments are locked, and new write operations roll over to a new write-cache segment. The data in the now-locked cache segment is destaged to the HDD capacity layer of the nodes for a hybrid system or to the SDD capacity layer of the nodes for an all-flash system. During the destaging process, data is deduplicated before being written to the capacity storage layer, and the resulting data can now be written to the HDDs or SDDs of the server. On hybrid systems, the now deduplicated and compressed data is also written to the dedicated read-cache area of the caching SSD, which speeds up read requests for data that has recently been written. When the data is destaged to an HDD, it is written in a single sequential operation, avoiding disk-head seek thrashing on the spinning disks and accomplishing the task in a minimal amount of time. Deduplication, compression, and destaging take place with no delays or I/O penalties for the guest virtual machines making requests to read or write data, which benefits both the HDD and SDD configurations.

For data read operations, data may be read from multiple locations. For data that was very recently written, the data is likely to still exist in the write log of the local platform controller memory or in the write log of the local caching-layer disk. If local write logs do not contain the data, the distributed file system metadata will be queried to see if the data is cached elsewhere, either in write logs of remote nodes or in the dedicated read-cache area of the local and remote caching SSDs of hybrid nodes. Finally, if the data has not been accessed in a significant amount of time, the file system will retrieve the requested data from the distributed capacity layer. As requests for read operations are made to the distributed file system and the data is retrieved from the capacity layer, the caching SSDs of hybrid nodes populate their dedicated read-cache area to speed up subsequent requests for the same data. All-flash configurations, however, do not employ a dedicated read cache because such caching does not provide any performance benefit; the persistent data copy already resides on high-performance SSDs.

Cisco Tetration Analytics platform

Applications are among the most critical entities in a data center. Organizations cannot always easily provide a secure infrastructure for applications without compromising agility. Today challenge is even more difficult to address because data centers are getting bigger and more complex, with hundreds or thousands of interdependent applications running in virtualized or containerized multicloud environments.

The Cisco Tetration Analytics platform addresses this operation and security challenge in a comprehensive way with multidimensional workload protection and application segmentation. It is a single platform that performs advanced analytics using an algorithmic approach and enforces a consistent whitelist policy for applications. This algorithmic approach includes unsupervised machine-learning techniques and behavioral analysis.

Cisco Tetration use cases

The Cisco Tetration platform provides a ready-to-use solution supporting the following use cases:

- Application behavior insight: Identify application components and their in-depth dependencies.
- Automated whitelist policy generation: Generate consistent whitelist policy based on application dependencies.
- Automated application segmentation: Provide effective application segmentation to enable efficient and secure zero-trust deployment. In addition, users can augment policies to limit application access based on users, user groups, and workload context.
- Automated policy enforcement: Provide consistent policy enforcement in a heterogeneous environment across on-premises data centers and private and public clouds.
- Policy compliance detection: Detect policy deviation in minutes and help ensure application-policy compliance.
- Server process behavior baseline and deviation reporting: Collect the complete process inventory along with process hash information, determine the baseline for the behavior, and identify deviations.

- Software inventory and vulnerability detection: Identify all the software packages and versions installed on the servers. Using the Common Vulnerabilities and Exposures (CVE) database, identify any associated vulnerabilities or exposures.
- Neighborhood graphing: Search for a specific application workspace and see a two-hops view of its communication with other servers within the data center.
- Forensic analysis: Use long-term data retention, with full details, for forensic analysis. (This capability is now extended to virtual desktop infrastructure [VDI] desktop virtual machines.)

Cisco Tetration sensors

To achieve these capabilities, Cisco Tetration uses a variety of sensors to collect telemetry data and communicate the flow information to the Cisco Tetration Analytics platform in real time. The telemetry data is collected from both servers and Cisco Nexus® switches. Table 1 lists the supported Cisco Tetration sensor types for a Tetration-V deployment.

Table 1. Cisco Tetration sensor types

Sensor type	Description	Where to install	When to apply	Supported by Tetration-V?
Software sensors	Software sensors are installed on the servers and collect telemetry data from every packet and every flow, process data, and the software packages installed. They also act as policy-enforcement points when enforcement is turned on.	The sensors are installed on the end servers (bare-metal servers, virtual machines, and containers). They are available for major distributions of Linux, Microsoft Windows servers, and Microsoft desktops (VDI use case only).	The use of these sensors is always the first option.	Yes
Cisco Encapsulated Remote Switched Port Analyzer (ERSPAN) sensors	These out-of-band sensors are designed to generate Cisco Tetration telemetry data using copies of the network packets. These sensors, when receiving ERSPAN packets, strip the ERSPAN header and generate Cisco Tetration telemetry data.	The copied network packets are delivered to out-of-band virtual machines running these sensors.	This approach can be used in parts of the network in which software and hardware sensors are not feasible.	Yes
F5 and Citrix sensors	These out-of-band sensors are designed to generate Cisco Tetration telemetry data using IPFIX from F5 and Citrix load balancers. Using this IPFIX telemetry, Tetration platform is able to stitch the client connections to specific servers when the request goes through the load balancers.	The IPFIX data is delivered to out-of-band virtual machines running these sensors.	This approach can be used to augment telemetry to get additional context and visualization.	Yes
Cisco AnyConnect® network visibility module (NVM) proxy sensor	The sensors collect telemetry data from the Cisco AnyConnect client, enabling the NVM to provide visibility into network-connected devices and user behaviors. Workload protection can be enforced on the collected user and user group information.	These sensors are on endpoint devices such as laptops, desktops, and smartphones on which the Cisco AnyConnect NVM agent is running.	Use this approach when a Cisco AnyConnect client is installed so that the NVM module can be enabled with no additional agent.	Yes

Note: Refer to the Cisco Tetration Platform data sheet for a full list of supported sensors and the operating systems for the software sensors.

Cisco Tetration deployment options

The Cisco Tetration platform provides an appliance-like experience. It provides flexible deployment options based on the data center size and whether the customer wants a deployment based on on-premises hardware or a public cloud. Three deployment options currently are available (Figure 7):

- Cisco Tetration Analytics platform (LFF) option and Cisco Tetration-M (SFF) option
- Cisco Tetration SaaS option
- Cisco Tetration Virtual (Tetration-V) option

Figure 7. Cisco Tetration platform deployment options

Deployment options

Tetration Appliance (Tetration, Tetration-M)

- Holistic data center workload protection and network performance features
- Support on-premises, public and private cloud
- Retain data for up to a year with Tetration and up to months with Tetration-M
- Tetration scales up to 25,000 workloads (VMs/Bare-metal). Tetration-M scales up to 5,000 workloads (VMs/Baremetal).
- Web GUI, REST API, push events and Tetration Apps

Tetration-V

- Supports virtual appliance-based deployment in ESXi-based environments or any on-premises hardware
- Offers holistic workload protection features
- Scales up to 1,000 servers
- Data retention: Weeks (subject to traffic volume)
- Web GUI, REST API, push events, and Tetration Apps

Tetration-SaaS

- Offers workload protection features without any on-premises hardware requirements
- Protect on-premises, public, and private cloud workloads
- Scales up to 25,000 workloads
- Data retention for months
- Faster onboarding to realize the benefits of the platform quickly

The Tetration-V option allows you to deploy the Cisco Tetration platform on your premises using the hardware of your choice. The Tetration-V version with VMware ESXi is well-suited for small-scale deployments and for data centers that host fewer than 1000 workloads (virtual machines or bare-metal servers). The solution validated in this document is for Cisco Tetration-V with VMware ESXi installed on Cisco HyperFlex systems.

Cisco Tetration-V on Cisco HyperFlex systems

The Cisco Tetration platform is powered by big-data technologies to support data center scale. It can process comprehensive telemetry information received from sensors in near-real time. The platform can enforce consistent policy across many applications running on thousands of servers in the data center. It is designed for long-term data retention, and it can search all the telemetry records from its data lake and return actionable insights in seconds. Although the Tetration-V on ESXi model is designed for smaller-scale deployments, the underlying storage infrastructure still must meet rigorous requirements to run Tetration-V in a sufficient and efficient way.

Cisco Tetration-V for VMware ESXi requirements

Table 2 lists the requirements for deploying the Cisco Tetration virtual appliance in an ESXi environment.

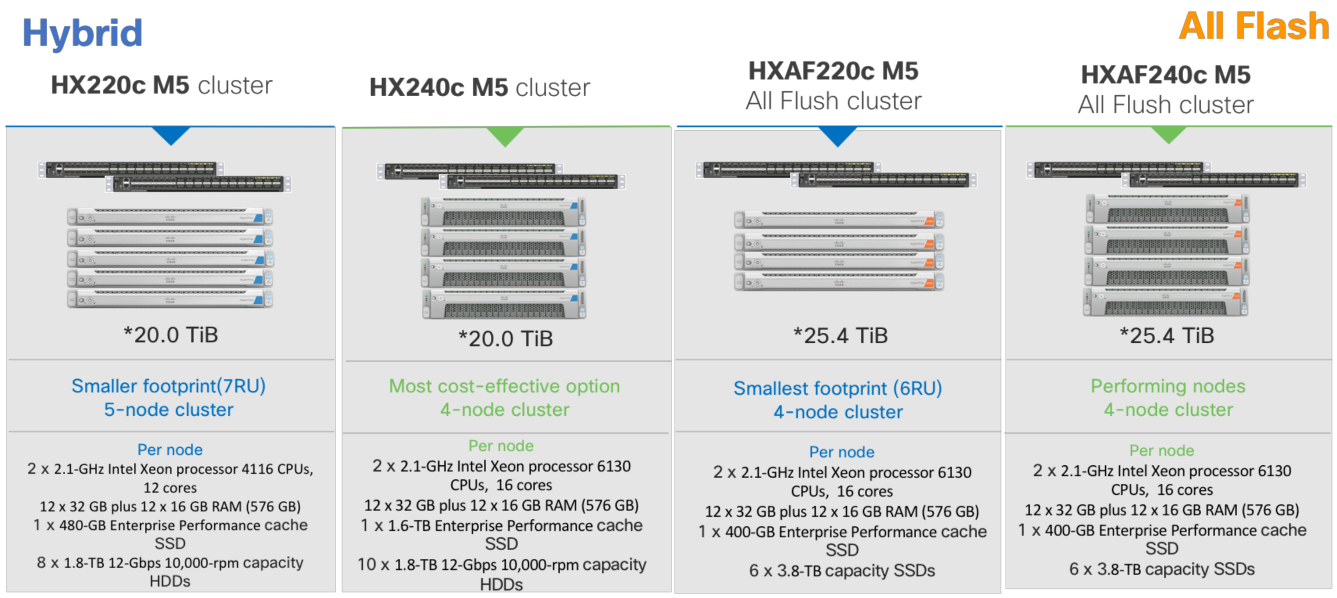
Table 2. Prerequisites for running the Cisco Tetration-V appliance

Components	Prerequisites		Notes
Software	• VMware cluster running VMware vSphere 6.5 • Capability to access the VMware vSphere Flash Player GUI • Cisco Tetration Analytics software-only orchestrator appliance .ova file • Cisco Tetration Analytics mother Red Hat Package Manager (RPM), adhoc RPM, and rpminstall RPM		
Hardware	CPU	Minimum 128 cores	Note that the requirement is cores, not hyperthreads.
	RAM	Minimum 2 TB	Some virtual machines need up to 128 GB of memory.
	Storage	• Minimum 18.1-TB capacity • Single durable data store • Capability to handle 5000 I/O operations per second (IOPs)	The single storage data store must be accessible from all nodes in the cluster.
Network	Minimum 10-Gbps connectivity between the virtual machines		
	Three virtual networks are required for deployment: • Public network: Dedicated or shared public network for external cluster traffic that must be reachable from sensors and clients; this network is used for Cisco Tetration Analytics GUI access • Private network: Dedicated nonroutable private network for internal cluster communication • Configuration network: Temporary network for a bootstrapping cluster that must be reachable from the user who is performing the deployment and that must have access to VMware vCenter; this network is used for Cisco Tetration Analytics setup GUI access		The configuration network should be a separate subnet from the public subnet and should be shut down after the deployment is complete.

Reference Cisco HyperFlex configuration

Cisco HyperFlex systems consolidate computing, networking, and storage resources in one easy-to-consume unit that enables an appliance-like Tetration-V platform to be built. Using Cisco HyperFlex software innovations, Cisco HyperFlex systems deliver a simplified solution with industry-leading performance, independent scaling, continuous storage optimization, and complete hyperconvergence in one system. Cisco HyperFlex systems enable multicloud IT support for any application of any scale. With a carefully selected Cisco HyperFlex configuration, Cisco Tetration virtual appliance bundles provide powerful data analytics and communication capabilities with a blend of deep storage and efficient data retrieval speed. Figure 8 lists the minimum Cisco HyperFlex M5 configuration that meets Tetration-V hardware requirements.

Figure 8. Minimum Cisco HyperFlex M5 configuration for Cisco Tetration-V



Hybrid

HX220c M5 cluster

*20.0 TiB

Smaller footprint(7RU)
5-node cluster

Per node
2 x 2.1-GHz Intel Xeon processor 4116 CPUs, 12 cores
12 x 32 GB plus 12 x 16 GB RAM (576 GB)
1 x 480-GB Enterprise Performance cache SSD
8 x 1.8-TB 12-Gbps 10,000-rpm capacity HDDs

HX240c M5 cluster

*20.0 TiB

Most cost-effective option
4-node cluster

Per node
2 x 2.1-GHz Intel Xeon processor 6130 CPUs, 16 cores
12 x 32 GB plus 12 x 16 GB RAM (576 GB)
1 x 1.6-TB Enterprise Performance cache SSD
10 x 1.8-TB 12-Gbps 10,000-rpm capacity HDDs

All Flash

HXAF220c M5
All Flush cluster

*25.4 TiB

Smallest footprint (6RU)
4-node cluster

Per node
2 x 2.1-GHz Intel Xeon processor 6130 CPUs, 16 cores
12 x 32 GB plus 12 x 16 GB RAM (576 GB)
1 x 400-GB Enterprise Performance cache SSD
6 x 3.8-TB capacity SSDs

HXAF240c M5
All Flush cluster

*25.4 TiB

Performing nodes
4-node cluster

Per node
2 x 2.1-GHz Intel Xeon processor 6130 CPUs, 16 cores
12 x 32 GB plus 12 x 16 GB RAM (576 GB)
1 x 400-GB Enterprise Performance cache SSD
6 x 3.8-TB capacity SSDs

*Usable capacity w/ RF3 before compression and deduplication

Test environment

This section introduces the technologies used in validating the solution described in this document.

The solution was tested with a 4-node HX220c M5SX All Flash cluster (Figure 9).

Figure 9. Cisco HyperFlex cluster used for testing

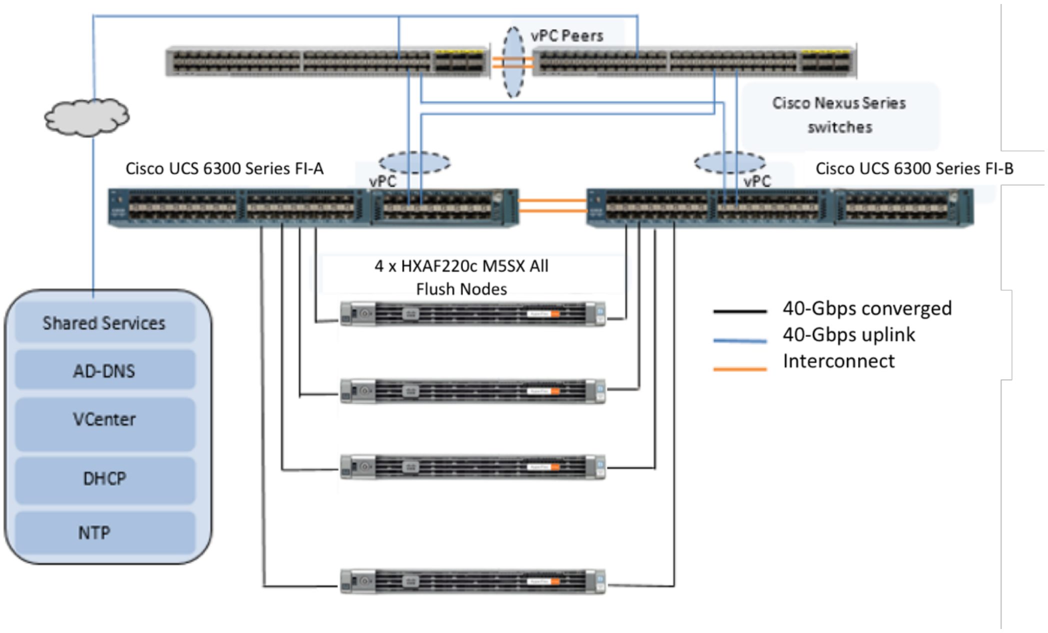

vPC Peers
Cisco Nexus Series switches
Cisco UCS 6300 Series FI-A
vPC
vPC
Cisco UCS 6300 Series FI-B
4 x HXAF220c M5SX All Flush Nodes
Shared Services
AD-DNS
VCenter
DHCP
NTP
40-Gbps converged
40-Gbps uplink
Interconnect

Table 3 lists the node specifications.

Table 3. Cisco HyperFlex HX220c M5SX All Flash Node specifications

Components	Specifications	Notes
CPU	2 x Intel Xeon Gold processor 6154 CPUs	2 x 18 cores
Memory	12 x 32-GB plus 12 x 16-GB DDR4 2666-MHz RDIMMs	576 GB
SSD	1 x 240-GB M.2 6-GB SATA SSD	Boot drive
	1 x 240-GB 2.5-inch Enterprise Value 6-GB SATA SSD	Housekeeping
	1 x 1.6-TB 2.5-inch NVMe High-Performance High-Endurance SSD	Configured as cache
	6 x 3.8-TB 2.5-inch Enterprise Value 6-GB SATA SSDs	Capacity disks for each node

Table 4 lists the software versions used in the test environment described in this document.

Table 4. Test environment versions

Layer	Device	Image
Computing	Cisco UCS 6332-16UP Fabric Interconnect pair	Release 3.2(3h)
	Cisco HyperFlex HX220c M5SX All Flash Node	Release 3.2(3h)
Network	Cisco Nexus 9372PX Switch pair (HX-Series upstream)	Release 7.0(3)I4(7)
Software	Cisco UCS Manager	Release 3.2(3h)
	Cisco HyperFlex Data Platform software	Release 3.0(1e)
	Cisco Tetration OS (software-only virtual appliance for installation)	Release 2.3.1.41
	Cisco Tetration OS upgrade patch	Release 2.3.1.51
	VMWare vSphere ESXi	Release 6.5.0, 8294253
	VMWare vSphere vCenter	Release 6.5.0.20000

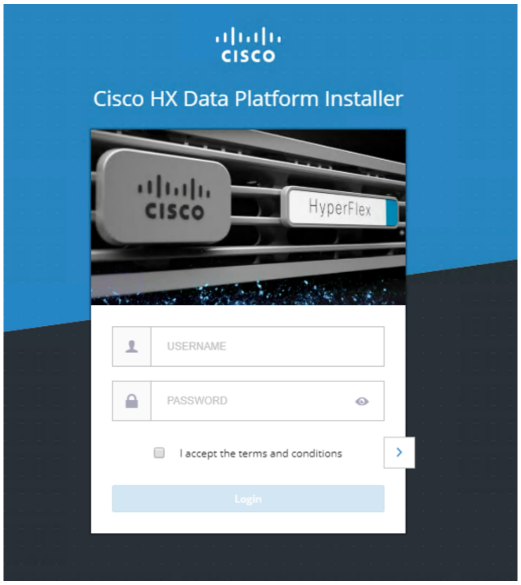
Cisco HyperFlex installation (nested VMware vCenter)

Use the following procedures to configure the Cisco HyperFlex system to run the Cisco Tetration virtual appliance software (Tetration-V) to provide a solid data analytics solution for small-scale virtualized environments. The procedures describe how to deploy and run an HX Data Platform configuration that has a vCenter virtual machine running on the Cisco HyperFlex storage cluster, rather than on a server external to the Cisco HyperFlex storage cluster. Although embedded VMware vSphere vCenter is recommended for this solution, use of an existing vCenter appliance on an external ESXi host or cluster is supported.

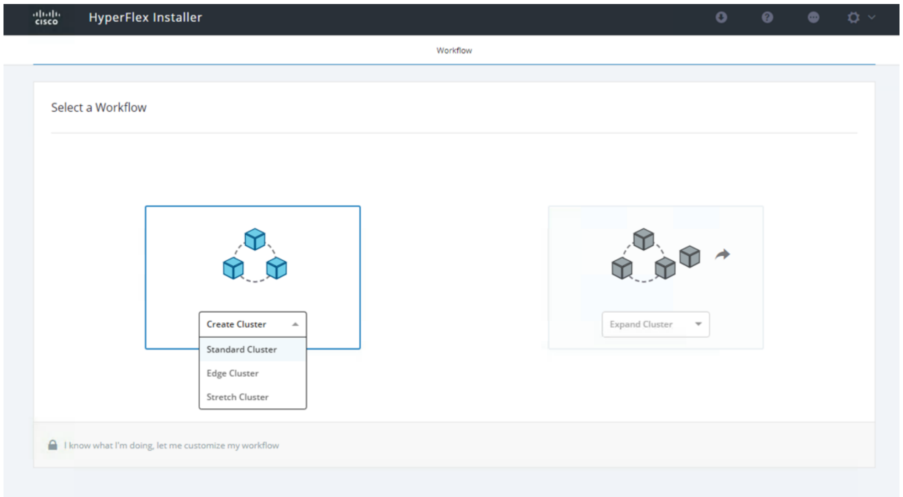
Installing Cisco HyperFlex systems

Follow the steps here to create a Cisco HyperFlex cluster. Definition of vCenter is a post-installation task.

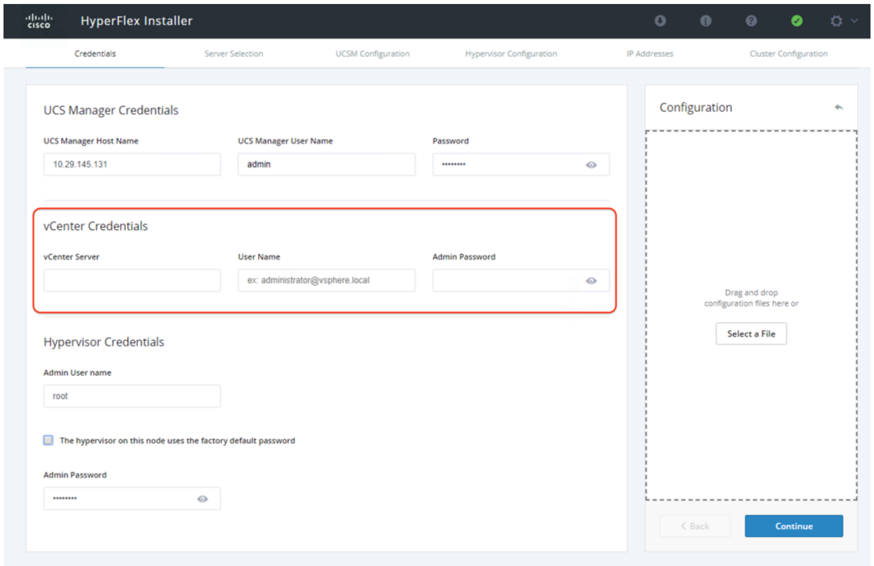
1. Download the HX Data Platform Installer OVA file from the Cisco website. Deploy the installer OVA file on a virtual machine in an existing VMware vSphere, VMware Workstation, VMware Fusion, or other virtualization environment that supports the import of OVA files.
2. Open the HX Data Platform Installer in a local web browser and accept the end-user license agreement.
3. Log in to the HX Data Platform Installer using the default root user name and password.


Cisco HX Data Platform Installer
HyperFlex
USERNAME
PASSWORD
I accept the terms and conditions
Login

4. On the Workflow page, choose Create Cluster > Standard Cluster.



5. On the Credentials page, enter the Cisco UCS Manager and HX Data Platform hypervisor credentials. Leave all three vCenter fields blank; the vCenter server will be registered in a post-installation task. Click Continue.



UCS Manager Credentials

UCS Manager Host Name: 10.29.145.131

UCS Manager User Name: admin

Password: ••••••••

vCenter Credentials

vCenter Server:

User Name: ex: administrator@vsphere.local

Admin Password:

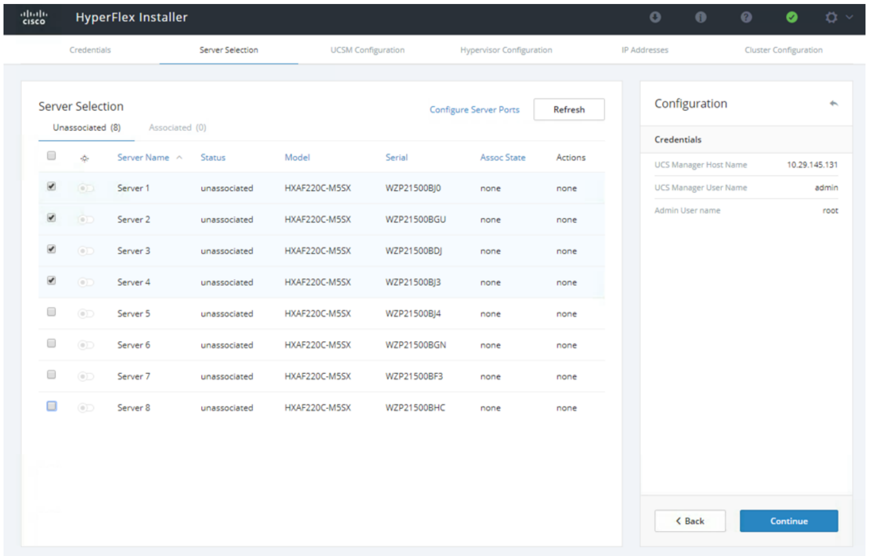
Hypervisor Credentials

Admin User name: root

☐ The hypervisor on this node uses the factory default password

Admin Password: ••••••••

6. Ignore the vCenter warning message and click Continue to confirm that the installation is being started without vCenter.
7. On the Server Selection page, under Unassociated, select the servers that you want to include in the Cisco HyperFlex storage cluster. Then click Continue.



Server Selection

Unassociated (8) Associated (0)

☐		Server Name	Status	Model	Serial	Assoc State	Actions
☑		Server 1	unassociated	HXAF220C-M5SX	WZP21500BJ0	none	none
☑		Server 2	unassociated	HXAF220C-M5SX	WZP21500BGU	none	none
☑		Server 3	unassociated	HXAF220C-M5SX	WZP21500BDJ	none	none
☑		Server 4	unassociated	HXAF220C-M5SX	WZP21500BJ3	none	none
☐		Server 5	unassociated	HXAF220C-M5SX	WZP21500BJ4	none	none
☐		Server 6	unassociated	HXAF220C-M5SX	WZP21500BGN	none	none
☐		Server 7	unassociated	HXAF220C-M5SX	WZP21500BF3	none	none
☐		Server 8	unassociated	HXAF220C-M5SX	WZP21500BHC	none	none

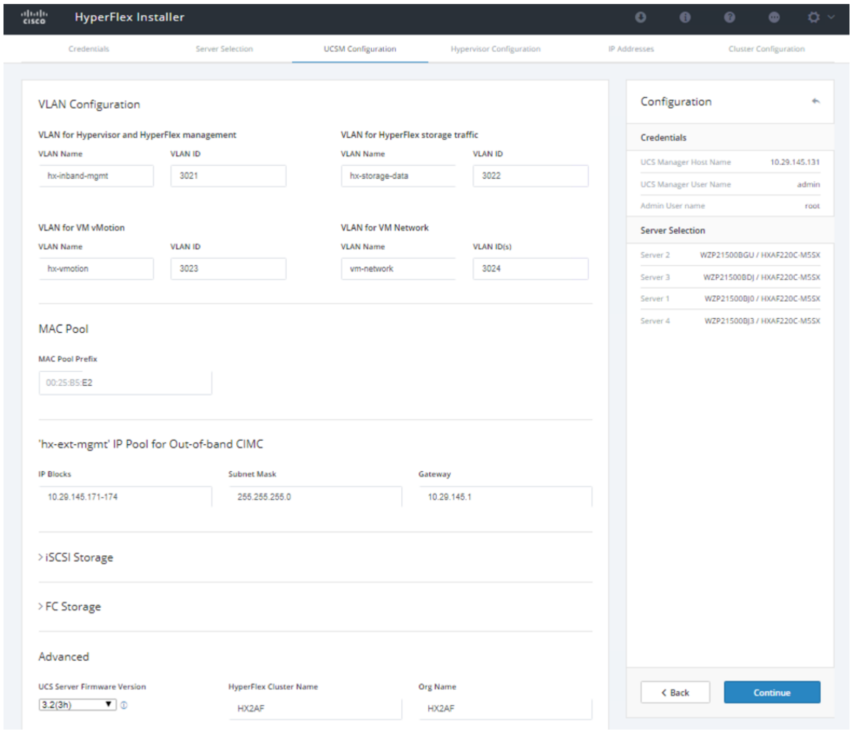
Configuration

Credentials

UCS Manager Host Name	10.29.145.131
UCS Manager User Name	admin
Admin User name	root

8. On the Cisco UCS Manager Configuration page, enter the Cisco UCS Manager configuration information and click Continue. Cisco UCS Manager configuration information includes the VLAN, MAC address pool, subnet, gateway, Small Computer System Interface over IP (iSCSI) storage, Fibre Channel storage, Cisco UCS firmware, Cisco HyperFlex cluster name, and organization name. Fill in these fields as required for any Cisco HyperFlex storage cluster. Then click Continue.

   You do not need to enable iSCSI or Fibre Channel storage in this step.



VLAN Configuration

VLAN for Hypervisor and HyperFlex management

VLAN Name	VLAN ID
hx-inband-mgmt	3021

VLAN for HyperFlex storage traffic

VLAN Name	VLAN ID
hx-storage-data	3022

VLAN for VM vMotion

VLAN Name	VLAN ID
hx-vmotion	3023

VLAN for VM Network

VLAN Name	VLAN ID(s)
vm-network	3024

MAC Pool

MAC Pool Prefix: 00:25:B5:E2

'hx-ext-mgmt' IP Pool for Out-of-band CIMC

IP Blocks	Subnet Mask	Gateway
10.29.145.171-174	255.255.255.0	10.29.145.1

› iSCSI Storage

› FC Storage

Advanced

UCS Server Firmware Version	HyperFlex Cluster Name	Org Name
3.2(3h)	HX2AF	HX2AF

Configuration

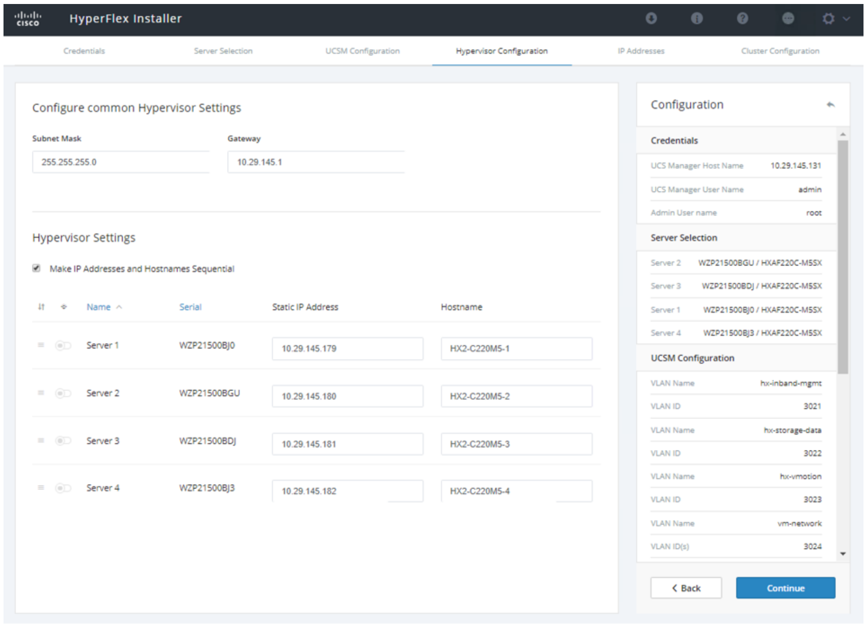
Credentials

UCS Manager Host Name	10.29.145.131
UCS Manager User Name	admin
Admin User name	root

Server Selection

Server 2	WZP21500BGU / HXAF220C-M5SX
Server 3	WZP21500BDJ / HXAF220C-M5SX
Server 1	WZP21500BJ0 / HXAF220C-M5SX
Server 4	WZP21500BJ3 / HXAF220C-M5SX

9. On the Hypervisor Configuration page, enter common hypervisor settings, such as the subnet mask, gateway, static IP addresses, and host names for the Cisco HyperFlex nodes. Then click Continue.



Configure common Hypervisor Settings

Subnet Mask	Gateway
255.255.255.0	10.29.145.1

Hypervisor Settings

☑ Make IP Addresses and Hostnames Sequential

Name	Serial	Static IP Address	Hostname
Server 1	WZP21500BJ0	10.29.145.179	HX2-C220M5-1
Server 2	WZP21500BGU	10.29.145.180	HX2-C220M5-2
Server 3	WZP21500BDJ	10.29.145.181	HX2-C220M5-3
Server 4	WZP21500BJ3	10.29.145.182	HX2-C220M5-4

Configuration

Credentials

UCS Manager Host Name	10.29.145.131
UCS Manager User Name	admin
Admin User name	root

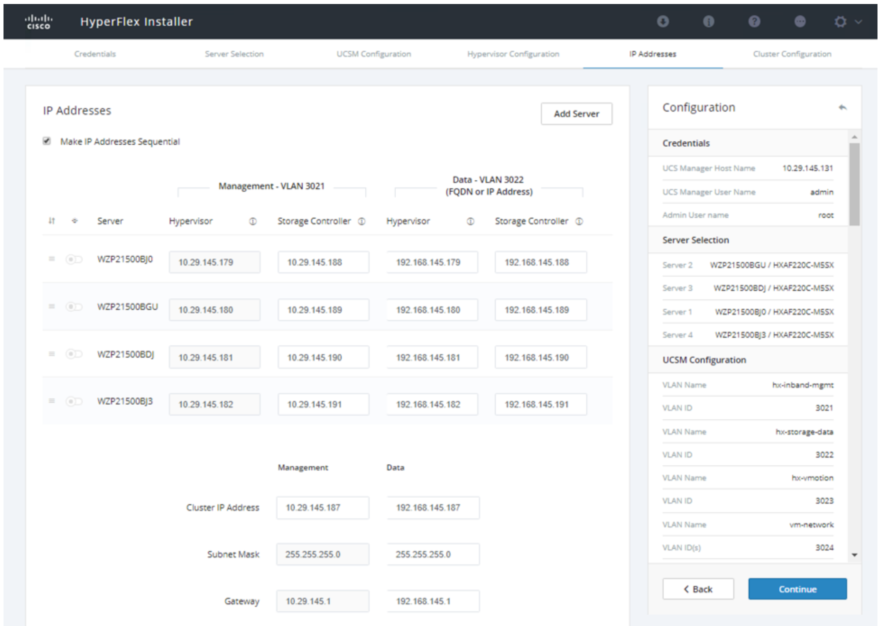
Server Selection

Server 2	WZP21500BGU / HXAF220C-M5SX
Server 3	WZP21500BDJ / HXAF220C-M5SX
Server 1	WZP21500BJ0 / HXAF220C-M5SX
Server 4	WZP21500BJ3 / HXAF220C-M5SX

UCSM Configuration

VLAN Name	hx-inband-mgmt
VLAN ID	3021
VLAN Name	hx-storage-data
VLAN ID	3022
VLAN Name	hx-vmotion
VLAN ID	3023
VLAN Name	vm-network
VLAN ID(s)	3024

10. On the IP Addresses page, for each Cisco HyperFlex node, complete the fields for hypervisor management, data IP addresses, subnet masks, and gateways. Specify the IP address settings for the Management network and the Data network.



IP Addresses

☑ Make IP Addresses Sequential

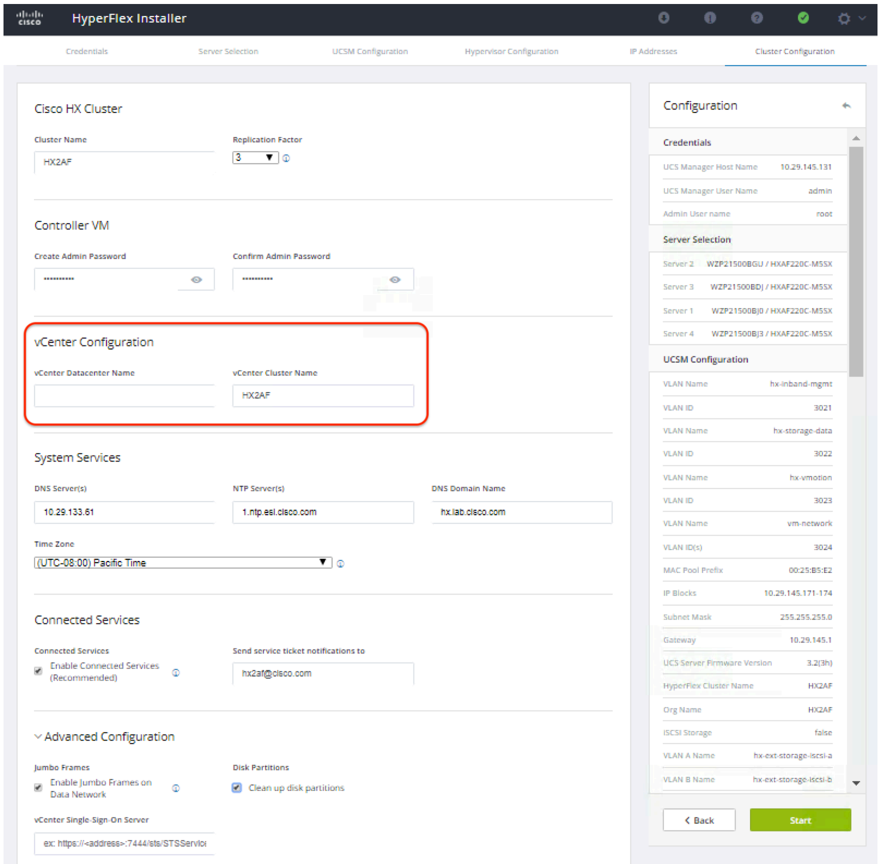
	Management - VLAN 3021		Data - VLAN 3022 (FQDN or IP Address)	
Server	Hypervisor	Storage Controller	Hypervisor	Storage Controller
WZP21500BJ0	10.29.145.179	10.29.145.188	192.168.145.179	192.168.145.188
WZP21500BGU	10.29.145.180	10.29.145.189	192.168.145.180	192.168.145.189
WZP21500BDJ	10.29.145.181	10.29.145.190	192.168.145.181	192.168.145.190
WZP21500BJ3	10.29.145.182	10.29.145.191	192.168.145.182	192.168.145.191

	Management	Data
Cluster IP Address	10.29.145.187	192.168.145.187
Subnet Mask	255.255.255.0	255.255.255.0
Gateway	10.29.145.1	192.168.145.1

Configuration

Credentials	
UCS Manager Host Name	10.29.145.131
UCS Manager User Name	admin
Admin User name	root
Server Selection	
Server 2	WZP21500BGU / HXAF220C-M5SX
Server 3	WZP21500BDJ / HXAF220C-M5SX
Server 1	WZP21500BJ0 / HXAF220C-M5SX
Server 4	WZP21500BJ3 / HXAF220C-M5SX
UCSM Configuration	
VLAN Name	hx-inband-mgmt
VLAN ID	3021
VLAN Name	hx-storage-data
VLAN ID	3022
VLAN Name	hx-vmotion
VLAN ID	3023
VLAN Name	vm-network
VLAN ID(s)	3024

11. On the Cluster Configuration page, enter the Cisco HyperFlex storage cluster settings, such as the storage cluster name, controller virtual machine credentials, data replication factor, DNS and NTP servers, and autosupport (ASUP). At this step, set RF = 3. Skip the vCenter configurations and leave the vCenter Datacenter Name field blank.



Cisco HX Cluster

Cluster Name: HX2AF

Replication Factor: 3

Controller VM

Create Admin Password: ••••••••••

Confirm Admin Password: ••••••••••

vCenter Configuration

vCenter Datacenter Name:

vCenter Cluster Name: HX2AF

System Services

DNS Server(s): 10.29.133.61

NTP Server(s): 1.ntp.esl.cisco.com

DNS Domain Name: hx.lab.cisco.com

Time Zone: (UTC-08:00) Pacific Time

Connected Services

Connected Services: ☑ Enable Connected Services (Recommended)

Send service ticket notifications to: hx2af@cisco.com

Advanced Configuration

Jumbo Frames: ☑ Enable Jumbo Frames on Data Network

Disk Partitions: ☑ Clean up disk partitions

vCenter Single-Sign-On Server: ex: https://<address>:7444/sts/STSServic

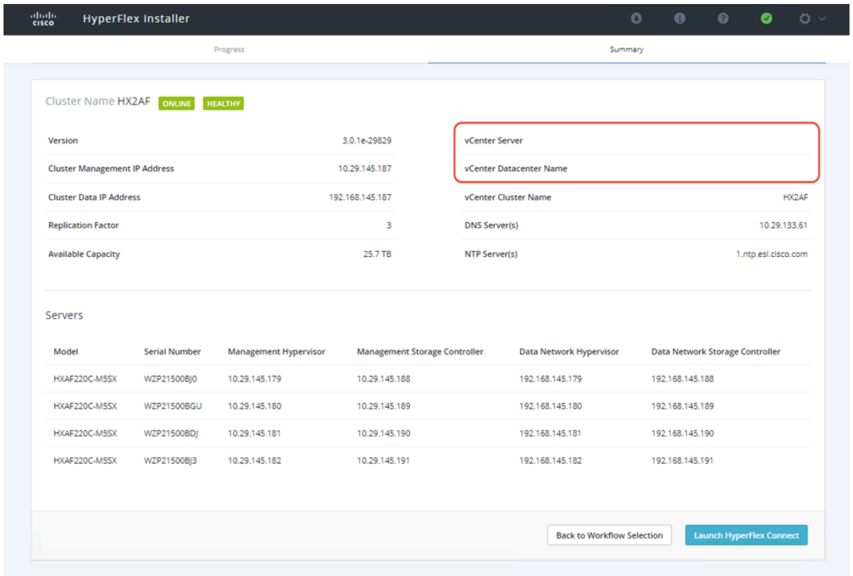
Configuration

Credentials	
UCS Manager Host Name	10.29.145.131
UCS Manager User Name	admin
Admin User name	root
Server Selection	
Server 2	WZP21500BGU / HXAF220C-M5SX
Server 3	WZP21500BDJ / HXAF220C-M5SX
Server 1	WZP21500BJ0 / HXAF220C-M5SX
Server 4	WZP21500BJ3 / HXAF220C-M5SX
UCSM Configuration	
VLAN Name	hx-inband-mgmt
VLAN ID	3021
VLAN Name	hx-storage-data
VLAN ID	3022
VLAN Name	hx-vmotion
VLAN ID	3023
VLAN Name	vm-network
VLAN ID(s)	3024
MAC Pool Prefix	00:25:B5:E2
IP Blocks	10.29.145.171-174
Subnet Mask	255.255.255.0
Gateway	10.29.145.1
UCS Server Firmware Version	3.2(3h)
HyperFlex Cluster Name	HX2AF
Org Name	HX2AF
iSCSI Storage	false
VLAN A Name	hx-ext-storage-iscsi-a
VLAN B Name	hx-ext-storage-iscsi-b

12. Click Start to create the Cisco HyperFlex cluster.

Note: See the Cisco HyperFlex Systems Installation Guide for VMware ESXi for complete deployment and cluster creation steps.

13. Wait for the cluster creation process to complete and for the summary page to appear. Note that the vCenter Server information is not specified.



Cluster Name HX2AF ONLINE HEALTHY

Version	3.0.1e-29829	vCenter Server	
Cluster Management IP Address	10.29.145.187	vCenter Datacenter Name	
Cluster Data IP Address	192.168.145.187	vCenter Cluster Name	HX2AF
Replication Factor	3	DNS Server(s)	10.29.133.61
Available Capacity	25.7 TB	NTP Server(s)	1.ntp.esl.cisco.com

Servers

Model	Serial Number	Management Hypervisor	Management Storage Controller	Data Network Hypervisor	Data Network Storage Controller
HXAF220C-M5SX	WZP21500BJ0	10.29.145.179	10.29.145.188	192.168.145.179	192.168.145.188
HXAF220C-M5SX	WZP21500BGU	10.29.145.180	10.29.145.189	192.168.145.180	192.168.145.189
HXAF220C-M5SX	WZP21500BDJ	10.29.145.181	10.29.145.190	192.168.145.181	192.168.145.190
HXAF220C-M5SX	WZP21500BJ3	10.29.145.182	10.29.145.191	192.168.145.182	192.168.145.191

Configuring the data store

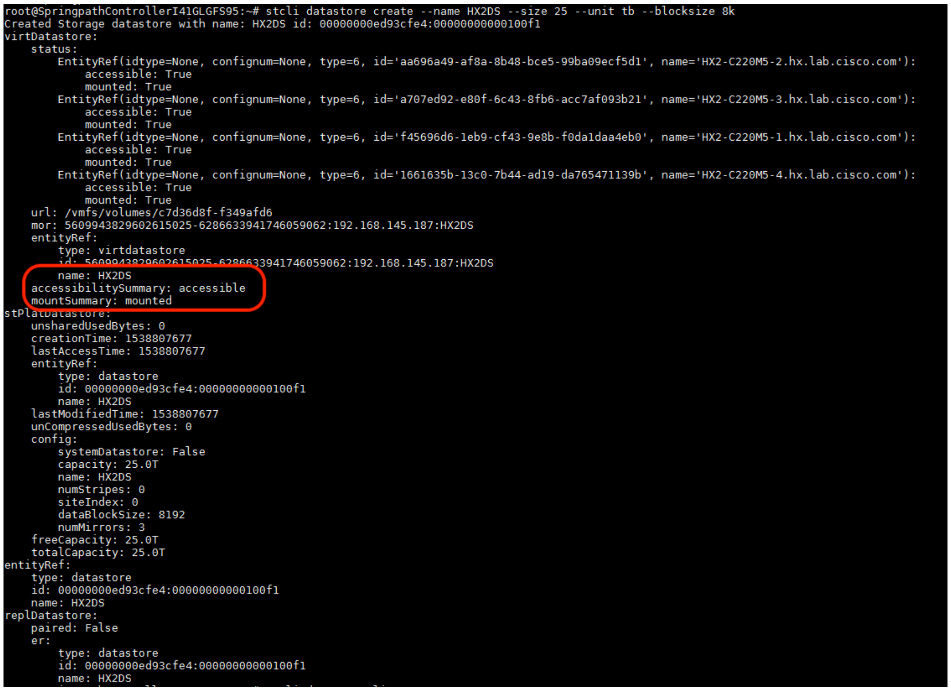
Use the following steps to configure the data stores for the Cisco HyperFlex storage cluster.

1. Log in to the cluster management IP address using Secure Shell SSH and the root credentials. Run the following command to create a large data store:

```
stcli datastore create --name <datastore name>  --size <size of datastore>  --unit {kb,mb,gb,tb}
--blocksize {8k,4k}
```

```
root@SpringpathCo...:~# stcli datastore create --name HX2DS --size 25 --unit tb --blocksize 8k
```

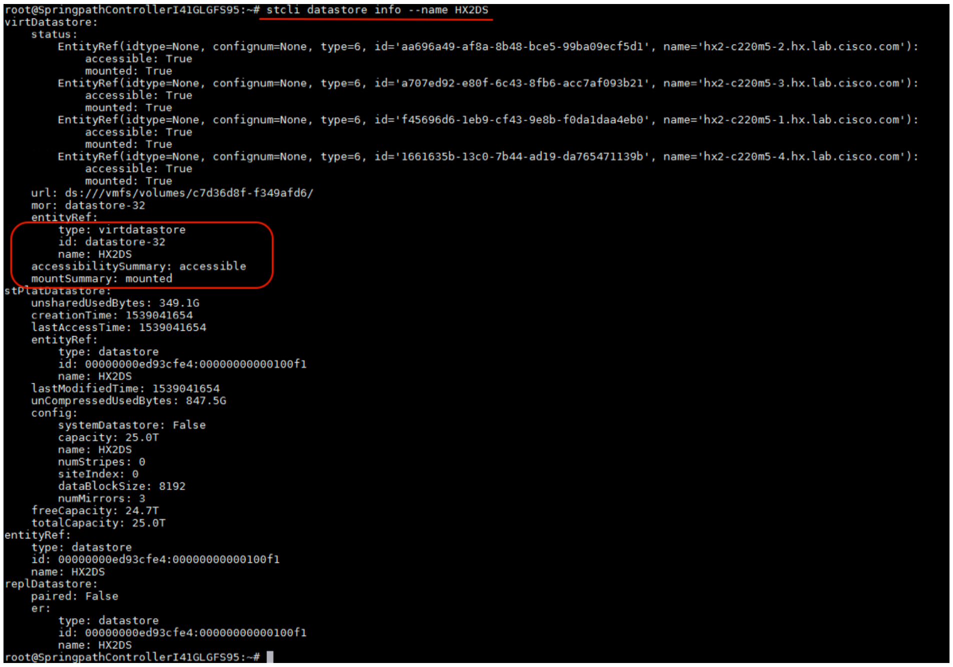
2. After the data store has been created successfully, check the data store status. Make sure that the data store shows the status **mountSummary: mounted** before continuing.



```
root@SpringpathControllerI41GLGFS95:~# stcli datastore create --name HX2DS --size 25 --unit tb --blocksize 8k
Created Storage datastore with name: HX2DS id: 00000000ed93cfe4:00000000000100f1
virtDatastore:
    status:
        EntityRef(idtype=None, confignum=None, type=6, id='aa696a49-af8a-8b48-bce5-99ba09ecf5d1', name='HX2-C220M5-2.hx.lab.cisco.com'):
            accessible: True
            mounted: True
        EntityRef(idtype=None, confignum=None, type=6, id='a707ed92-e80f-6c43-8fb6-acc7af093b21', name='HX2-C220M5-3.hx.lab.cisco.com'):
            accessible: True
            mounted: True
        EntityRef(idtype=None, confignum=None, type=6, id='f45696d6-1eb9-cf43-9e8b-f0da1daa4eb0', name='HX2-C220M5-1.hx.lab.cisco.com'):
            accessible: True
            mounted: True
        EntityRef(idtype=None, confignum=None, type=6, id='1661635b-13c0-7b44-ad19-da765471139b', name='HX2-C220M5-4.hx.lab.cisco.com'):
            accessible: True
            mounted: True
    url: /vmfs/volumes/c7d36d8f-f349afd6
    mor: 5609943829602615025-6286633941746059062:192.168.145.187:HX2DS
    entityRef:
        type: virtdatastore
        id: 5609943829602615025-6286633941746059062:192.168.145.187:HX2DS
        name: HX2DS
    accessibilitySummary: accessible
    mountSummary: mounted
stPlatDatastore:
    unsharedUsedBytes: 0
    creationTime: 1538807677
    lastAccessTime: 1538807677
    entityRef:
        type: datastore
        id: 00000000ed93cfe4:00000000000100f1
        name: HX2DS
    lastModifiedTime: 1538807677
    unCompressedUsedBytes: 0
    config:
        systemDatastore: False
        capacity: 25.0T
        name: HX2DS
        numStripes: 0
        siteIndex: 0
        dataBlockSize: 8192
        numMirrors: 3
    freeCapacity: 25.0T
    totalCapacity: 25.0T
entityRef:
    type: datastore
    id: 00000000ed93cfe4:00000000000100f1
    name: HX2DS
replDatastore:
    paired: False
    er:
        type: datastore
        id: 00000000ed93cfe4:00000000000100f1
        name: HX2DS
```

You can also run the following command to check the data store status:

```
root@SpringpathCo...:~# stcli datastore info --name HX2DS
```

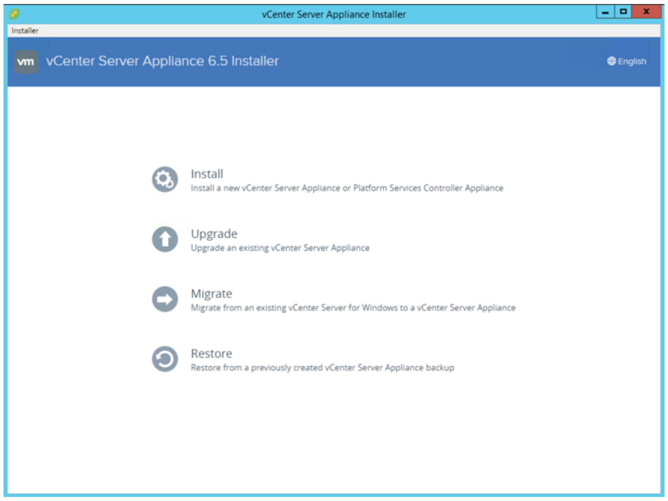


```
root@SpringpathControllerI41GLGFS95:~# stcli datastore info --name HX2DS
virtDatastore:
    status:
        EntityRef(idtype=None, confignum=None, type=6, id='aa696a49-af8a-8b48-bce5-99ba09ecf5d1', name='hx2-c220m5-2.hx.lab.cisco.com'):
            accessible: True
            mounted: True
        EntityRef(idtype=None, confignum=None, type=6, id='a707ed92-e80f-6c43-8fb6-acc7af093b21', name='hx2-c220m5-3.hx.lab.cisco.com'):
            accessible: True
            mounted: True
        EntityRef(idtype=None, confignum=None, type=6, id='f45696d6-1eb9-cf43-9e8b-f0da1daa4eb0', name='hx2-c220m5-1.hx.lab.cisco.com'):
            accessible: True
            mounted: True
        EntityRef(idtype=None, confignum=None, type=6, id='1661635b-13c0-7b44-ad19-da765471139b', name='hx2-c220m5-4.hx.lab.cisco.com'):
            accessible: True
            mounted: True
    url: ds:///vmfs/volumes/c7d36d8f-f349afd6/
    mor: datastore-32
    entityRef:
        type: virtdatastore
        id: datastore-32
        name: HX2DS
    accessibilitySummary: accessible
    mountSummary: mounted
stPlatDatastore:
    unsharedUsedBytes: 349.1G
    creationTime: 1539041654
    lastAccessTime: 1539041654
    entityRef:
        type: datastore
        id: 00000000ed93cfe4:00000000000100f1
        name: HX2DS
    lastModifiedTime: 1539041654
    unCompressedUsedBytes: 847.5G
    config:
        systemDatastore: False
        capacity: 25.0T
        name: HX2DS
        numStripes: 0
        siteIndex: 0
        dataBlockSize: 8192
        numMirrors: 3
    freeCapacity: 24.7T
    totalCapacity: 25.0T
entityRef:
    type: datastore
    id: 00000000ed93cfe4:00000000000100f1
    name: HX2DS
replDatastore:
    paired: False
    er:
        type: datastore
        id: 00000000ed93cfe4:00000000000100f1
        name: HX2DS
root@SpringpathControllerI41GLGFS95:~#
```

Installing VMware vCenter

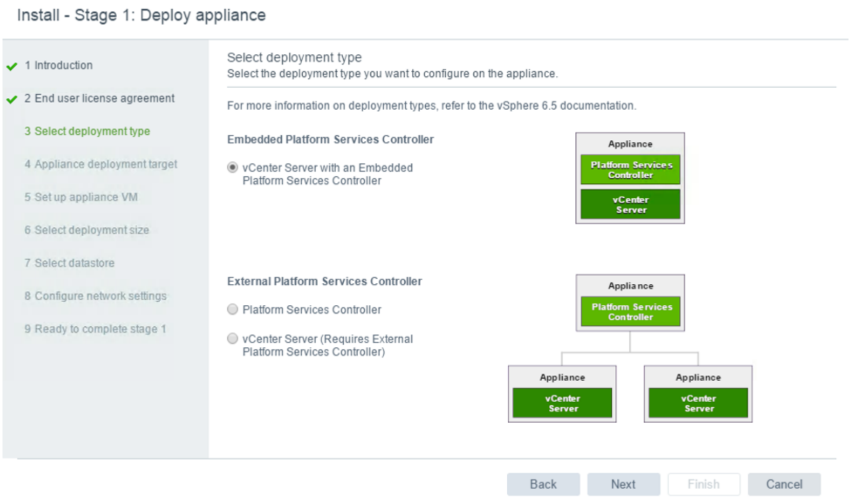
Use the following steps to install the embedded VMware vCenter Server appliance on the Cisco HyperFlex storage cluster.

1. Use the vCenter Server Appliance Installer wizard to build a new vCenter appliance virtual machine.



vCenter Server Appliance Installer
Installer
vm vCenter Server Appliance 6.5 Installer
English
Install
Install a new vCenter Server Appliance or Platform Services Controller Appliance
Upgrade
Upgrade an existing vCenter Server Appliance
Migrate
Migrate from an existing vCenter Server for Windows to a vCenter Server Appliance
Restore
Restore from a previously created vCenter Server Appliance backup

2. Review the introduction to stage 1 of the installation. Click Next.
3. Accept the terms of the license agreement. Click Next.
4. Choose to install vCenter with an embedded platform services controller. Click Next.



Install - Stage 1: Deploy appliance

- ✓ 1 Introduction
- ✓ 2 End user license agreement
- 3 Select deployment type
- 4 Appliance deployment target
- 5 Set up appliance VM
- 6 Select deployment size
- 7 Select datastore
- 8 Configure network settings
- 9 Ready to complete stage 1

Select deployment type
Select the deployment type you want to configure on the appliance.

For more information on deployment types, refer to the vSphere 6.5 documentation.

Embedded Platform Services Controller

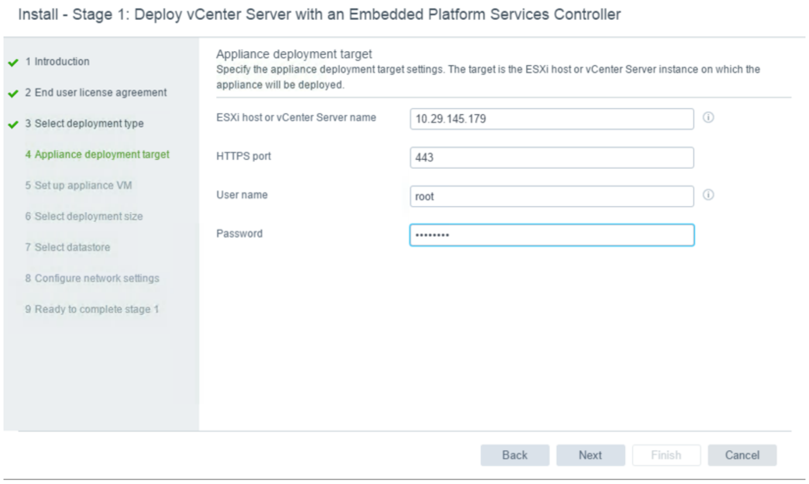
● vCenter Server with an Embedded Platform Services Controller

External Platform Services Controller

○ Platform Services Controller

○ vCenter Server (Requires External Platform Services Controller)

5. Deploy the new vCenter on any one of the Cisco HyperFlex servers in the cluster. Click Next.



Install - Stage 1: Deploy vCenter Server with an Embedded Platform Services Controller

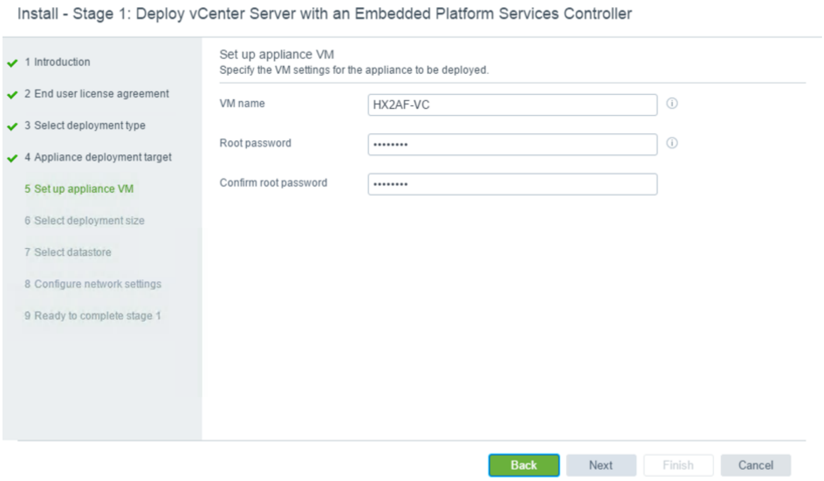
- ✓ 1 Introduction
- ✓ 2 End user license agreement
- ✓ 3 Select deployment type
- 4 Appliance deployment target
- 5 Set up appliance VM
- 6 Select deployment size
- 7 Select datastore
- 8 Configure network settings
- 9 Ready to complete stage 1

Appliance deployment target
Specify the appliance deployment target settings. The target is the ESXi host or vCenter Server instance on which the appliance will be deployed.

ESXi host or vCenter Server name	10.29.145.179
HTTPS port	443
User name	root
Password	••••••••

6. Ignore the certificate warning by clicking Yes.

7. Enter the virtual machine’s name and password. Click Next.



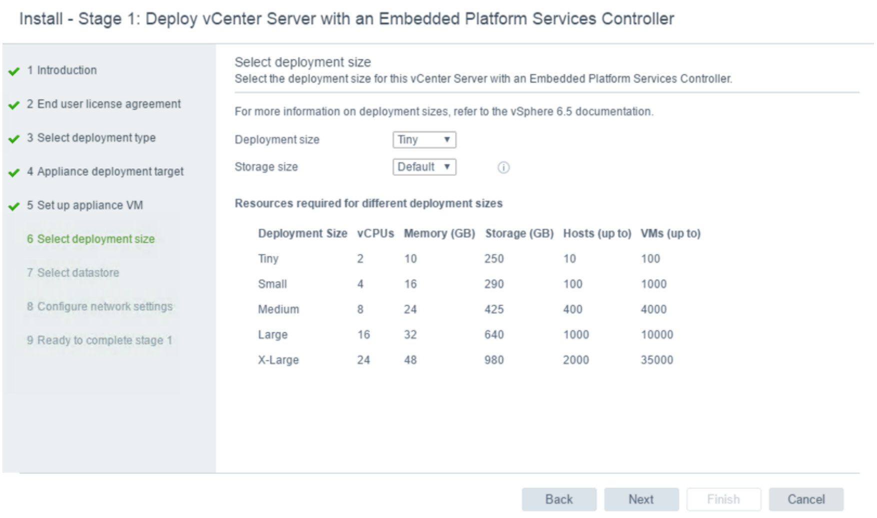
Install - Stage 1: Deploy vCenter Server with an Embedded Platform Services Controller

- ✓ 1 Introduction
- ✓ 2 End user license agreement
- ✓ 3 Select deployment type
- ✓ 4 Appliance deployment target
- 5 Set up appliance VM
- 6 Select deployment size
- 7 Select datastore
- 8 Configure network settings
- 9 Ready to complete stage 1

Set up appliance VM
Specify the VM settings for the appliance to be deployed.

VM name	HX2AF-VC
Root password	••••••••
Confirm root password	••••••••

8. Select the deployment size based on the manage needs of your environment. Click Next.



Install - Stage 1: Deploy vCenter Server with an Embedded Platform Services Controller

- ✓ 1 Introduction
- ✓ 2 End user license agreement
- ✓ 3 Select deployment type
- ✓ 4 Appliance deployment target
- ✓ 5 Set up appliance VM
- 6 Select deployment size
- 7 Select datastore
- 8 Configure network settings
- 9 Ready to complete stage 1

Select deployment size
Select the deployment size for this vCenter Server with an Embedded Platform Services Controller.

For more information on deployment sizes, refer to the vSphere 6.5 documentation.

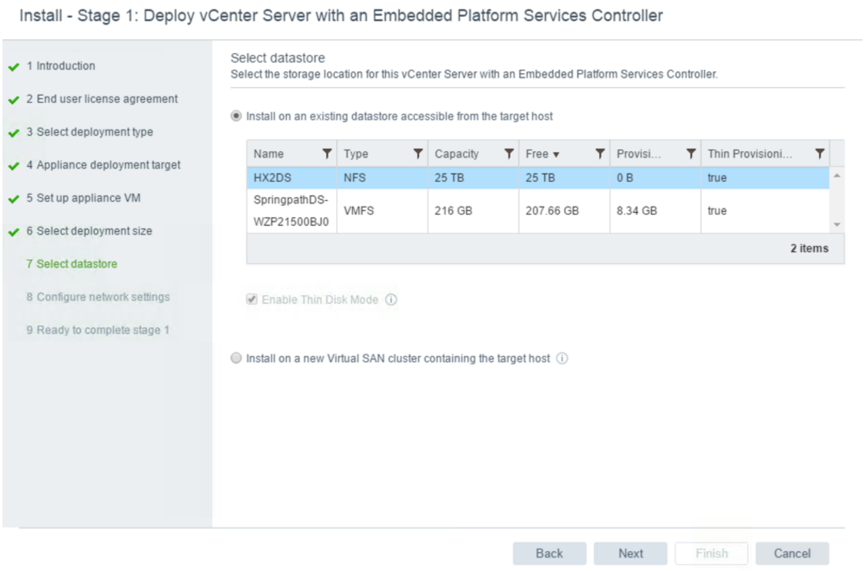
Deployment size: Tiny ▾

Storage size: Default ▾ ⓘ

Resources required for different deployment sizes

Deployment Size	vCPUs	Memory (GB)	Storage (GB)	Hosts (up to)	VMs (up to)
Tiny	2	10	250	10	100
Small	4	16	290	100	1000
Medium	8	24	425	400	4000
Large	16	32	640	1000	10000
X-Large	24	48	980	2000	35000

9. Use the newly created data store for persistent storage. Click Next.



Install - Stage 1: Deploy vCenter Server with an Embedded Platform Services Controller

- ✓ 1 Introduction
- ✓ 2 End user license agreement
- ✓ 3 Select deployment type
- ✓ 4 Appliance deployment target
- ✓ 5 Set up appliance VM
- ✓ 6 Select deployment size
- 7 Select datastore
- 8 Configure network settings
- 9 Ready to complete stage 1

Select datastore
Select the storage location for this vCenter Server with an Embedded Platform Services Controller.

● Install on an existing datastore accessible from the target host

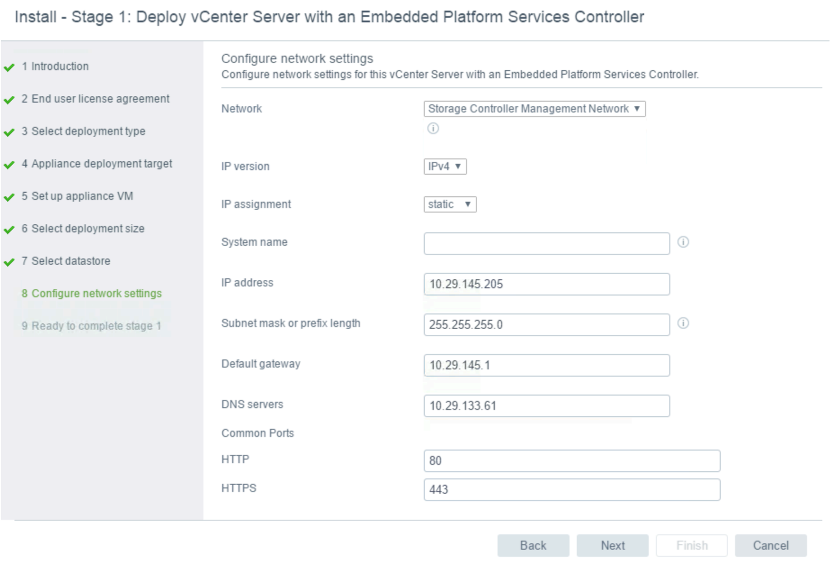
Name	Type	Capacity	Free ▾	Provisi...	Thin Provisioni...
HX2DS	NFS	25 TB	25 TB	0 B	true
SpringpathDS-WZP21500BJ0	VMFS	216 GB	207.66 GB	8.34 GB	true

2 items

☑ Enable Thin Disk Mode ⓘ

○ Install on a new Virtual SAN cluster containing the target host ⓘ

10. Select an appropriate port group for the network. The port group must have network access to the Cisco HyperFlex cluster management IP address and all ESXi management IP addresses. Specify Input the IP configuration. Click Next.



Install - Stage 1: Deploy vCenter Server with an Embedded Platform Services Controller

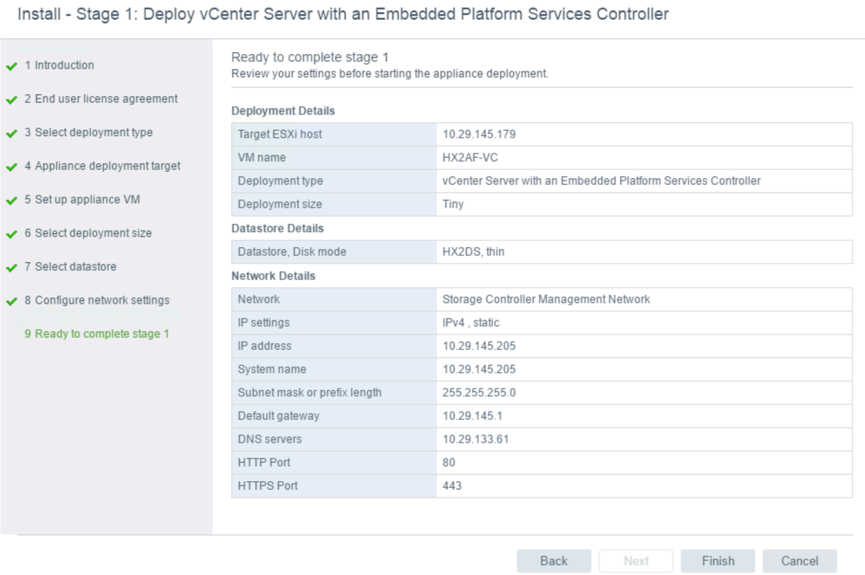
✓ 1 Introduction
✓ 2 End user license agreement
✓ 3 Select deployment type
✓ 4 Appliance deployment target
✓ 5 Set up appliance VM
✓ 6 Select deployment size
✓ 7 Select datastore
8 Configure network settings
9 Ready to complete stage 1

Configure network settings

Configure network settings for this vCenter Server with an Embedded Platform Services Controller.

Network	Storage Controller Management Network ▾
IP version	IPv4 ▾
IP assignment	static ▾
System name	
IP address	10.29.145.205
Subnet mask or prefix length	255.255.255.0
Default gateway	10.29.145.1
DNS servers	10.29.133.61
Common Ports	
HTTP	80
HTTPS	443

11. Review the configuration for your vCenter server appliance virtual machine. Click Finish to start the installation.



Install - Stage 1: Deploy vCenter Server with an Embedded Platform Services Controller

✓ 1 Introduction
✓ 2 End user license agreement
✓ 3 Select deployment type
✓ 4 Appliance deployment target
✓ 5 Set up appliance VM
✓ 6 Select deployment size
✓ 7 Select datastore
✓ 8 Configure network settings
9 Ready to complete stage 1

Ready to complete stage 1

Review your settings before starting the appliance deployment.

Deployment Details

Target ESXi host	10.29.145.179
VM name	HX2AF-VC
Deployment type	vCenter Server with an Embedded Platform Services Controller
Deployment size	Tiny

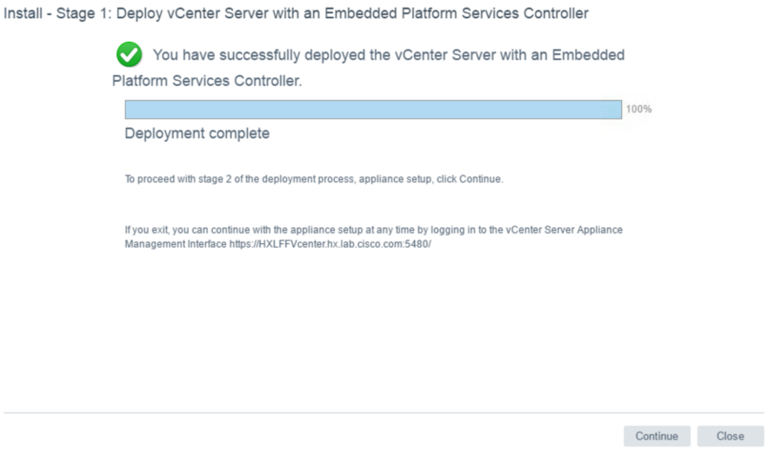
Datastore Details

Datastore, Disk mode	HX2DS, thin

Network Details

Network	Storage Controller Management Network
IP settings	IPv4 , static
IP address	10.29.145.205
System name	10.29.145.205
Subnet mask or prefix length	255.255.255.0
Default gateway	10.29.145.1
DNS servers	10.29.133.61
HTTP Port	80
HTTPS Port	443

12. When stage 1 deployment is complete, click Continue for stage 2 vCenter configuration.



Install - Stage 1: Deploy vCenter Server with an Embedded Platform Services Controller

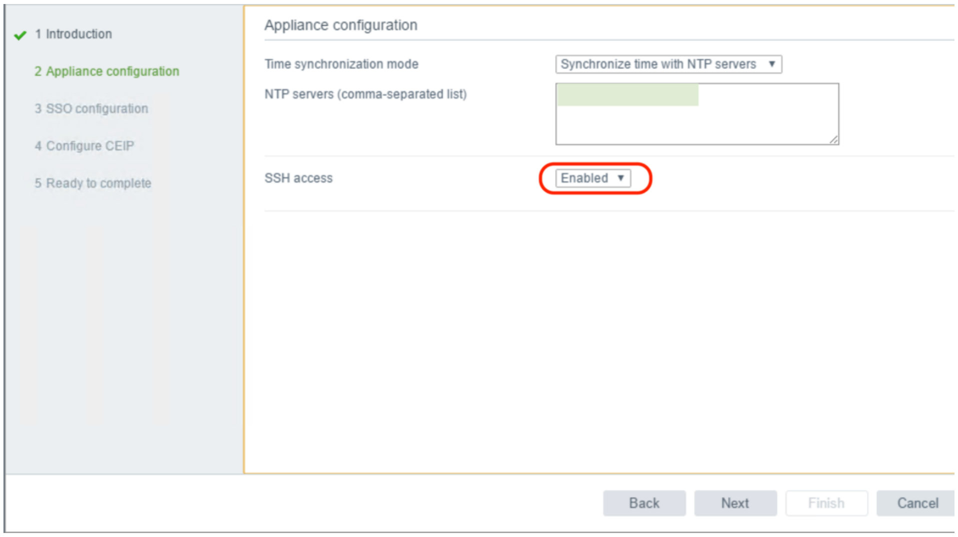
✓ You have successfully deployed the vCenter Server with an Embedded Platform Services Controller.

Deployment complete

To proceed with stage 2 of the deployment process, appliance setup, click Continue.

If you exit, you can continue with the appliance setup at any time by logging in to the vCenter Server Appliance Management Interface https://HXLFFVcenter.hx.lab.cisco.com:5480/

13. Review the introduction to stage 2 of the deployment process. Click Next.
14. Configure the NTP servers in the appliance and enable remote SSH access to allow high availability for VCenter. Click Next.



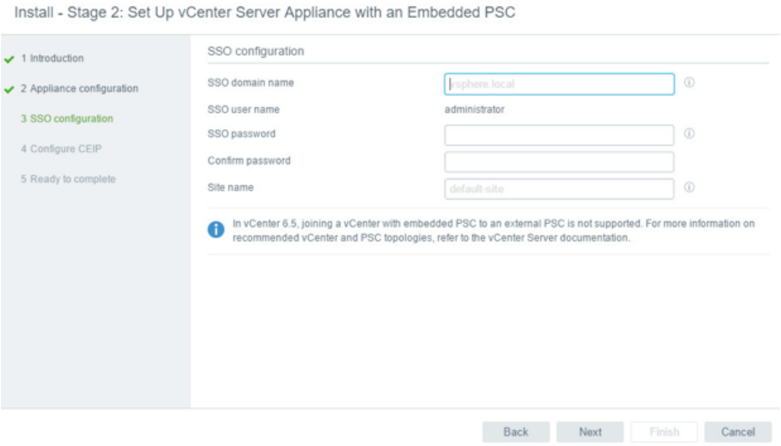
Appliance configuration

Time synchronization mode: Synchronize time with NTP servers ▾

NTP servers (comma-separated list)

SSH access: Enabled ▾

15. Create a new vCenter single sign-on (SSO) domain or join an existing domain. For example, enter vsphere.local as the domain name, set the password for the administrator account, and enter a default site name. Click Next.



Install - Stage 2: Set Up vCenter Server Appliance with an Embedded PSC

SSO configuration

SSO domain name: vsphere.local

SSO user name: administrator

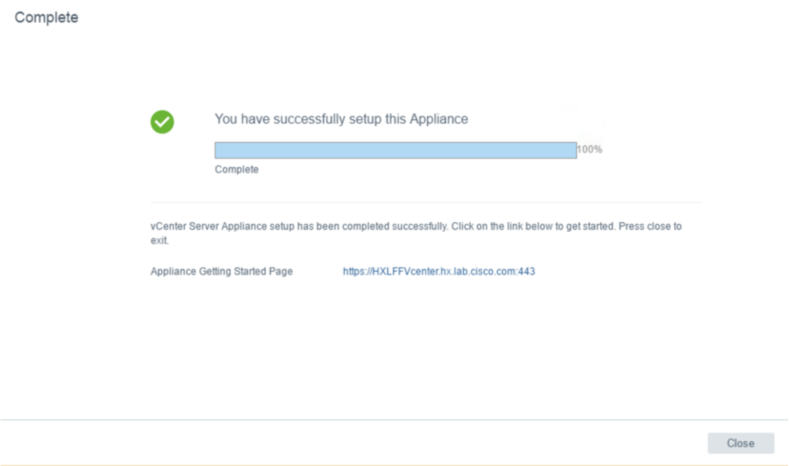
SSO password:

Confirm password:

Site name: default-site

In vCenter 6.5, joining a vCenter with embedded PSC to an external PSC is not supported. For more information on recommended vCenter and PSC topologies, refer to the vCenter Server documentation.

16. Review the VMware Customer Experience Improvement Program (CEIP) page and select or deselect the Join box. Click Next.
17. Review the settings on the Ready to Complete page and click Finish.
18. Click OK to complete stage 2 of the deployment process and set up the appliance.



Complete

You have successfully setup this Appliance

100%

Complete

vCenter Server Appliance setup has been completed successfully. Click on the link below to get started. Press close to exit.

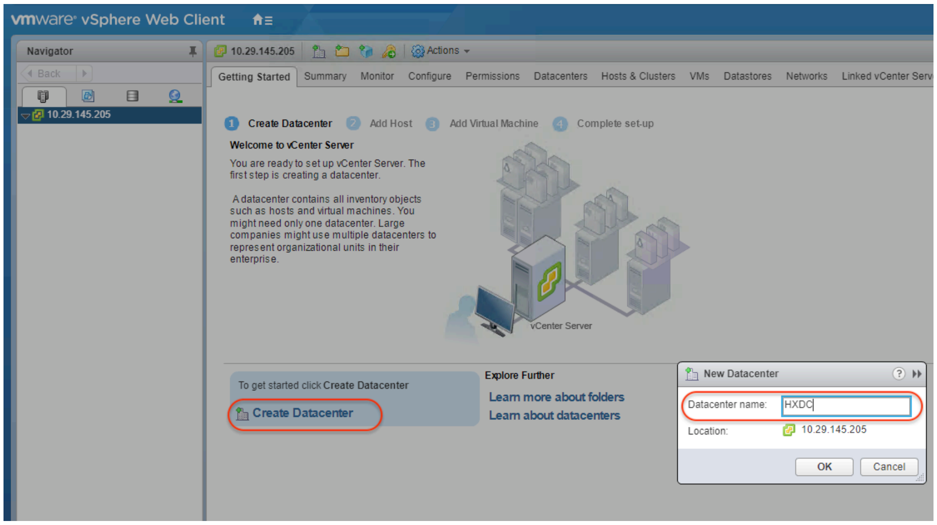
Appliance Getting Started Page https://HXLFFVcenter.hx.lab.cisco.com:443

19. When the deployment completes successfully, click Close to exit the installer wizard.

Configuring VMware vSphere

Use the following steps to configure the embedded VMware vSphere server to provide high availability for the Cisco Tetration virtual appliance.

1. After successfully deploying vCenter, log in to the vSphere Web Client. On the Getting Started page, choose Create Datacenter.
2. Enter the new data center name—for example, **HXDC**—and click OK.



Welcome to vCenter Server

You are ready to set up vCenter Server. The first step is creating a datacenter.

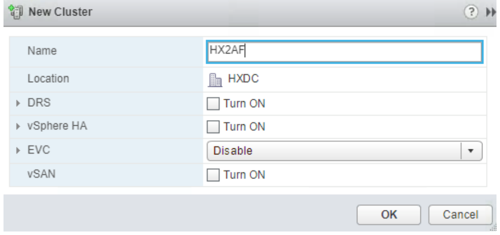
A datacenter contains all inventory objects such as hosts and virtual machines. You might need only one datacenter. Large companies might use multiple datacenters to represent organizational units in their enterprise.

To get started click Create Datacenter

Datacenter name: HXDC

Location: 10.29.145.205

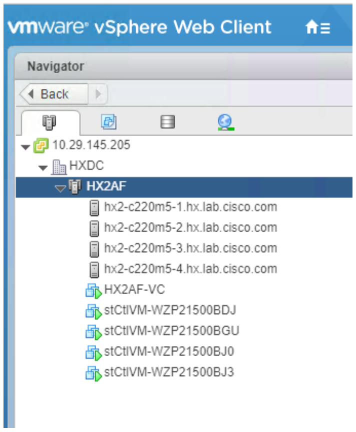
3. Create a new cluster in the new data center—for example, **HX2AF**—leaving high availability (HA) and VMware Distributed Resource Scheduler (DRS) disabled. They will be enabled later. Click OK.



New Cluster

Name	HX2AF
Location	HXDC
DRS	□ Turn ON
vSphere HA	□ Turn ON
EVC	Disable
vSAN	□ Turn ON

4. Right-click the newly created cluster and choose Add Host to manually add one Cisco HyperFlex server to the cluster.
    a. Enter the host name, root user, and password to connect the server.
    b. Assign an ESXi license, or use the evaluation license and assign a license later.
    c. Keep the default Lockdown mode.
    d. Review the settings and then click Finish to add the Cisco HyperFlex node.
5. Repeat step 4 to add all the Cisco HyperFlex servers to the Cisco HyperFlex cluster.


vmware vSphere Web Client
Navigator
Back
10.29.145.205
HXDC
HX2AF
hx2-c220m5-1.hx.lab.cisco.com
hx2-c220m5-2.hx.lab.cisco.com
hx2-c220m5-3.hx.lab.cisco.com
hx2-c220m5-4.hx.lab.cisco.com
HX2AF-VC
stCtlVM-WZP21500BDJ
stCtlVM-WZP21500BGU
stCtlVM-WZP21500BJ0
stCtlVM-WZP21500BJ3

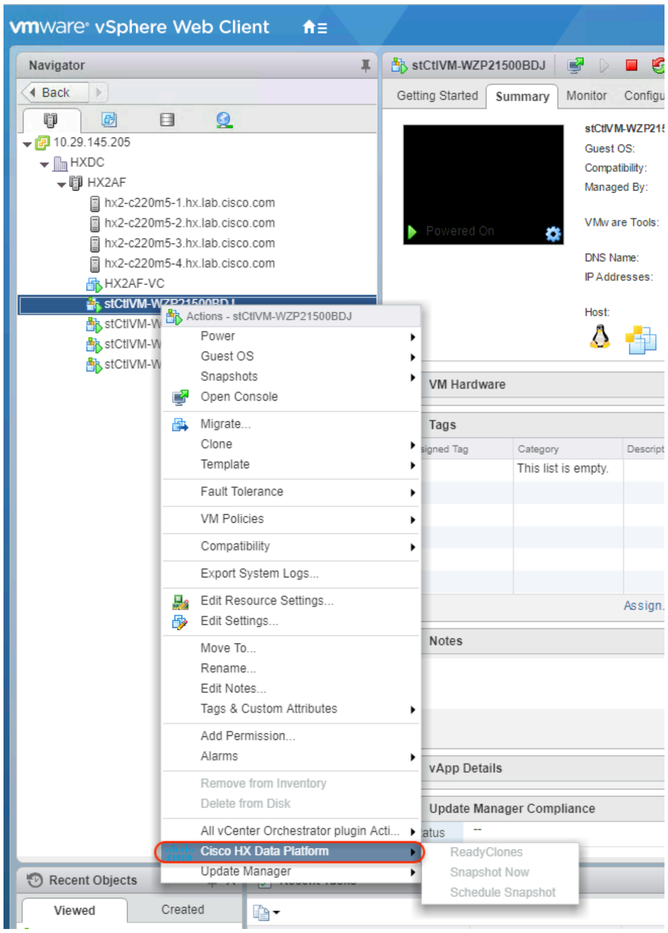
6. Log out of the vSphere Web Client.
7. Register the Cisco HyperFlex storage cluster to the newly configured vCenter server.
8. Log in to the Cisco HyperFlex cluster management IP address using SSH and the root credentials. Then run the following command:

```
stcli cluster reregister --vcenter-datacenter <Datacenter Name> --vcenter-cluster <Cluster Name>
--vcenter-url <URL or IP of vCenter> --vcenter-user <admin username>
```

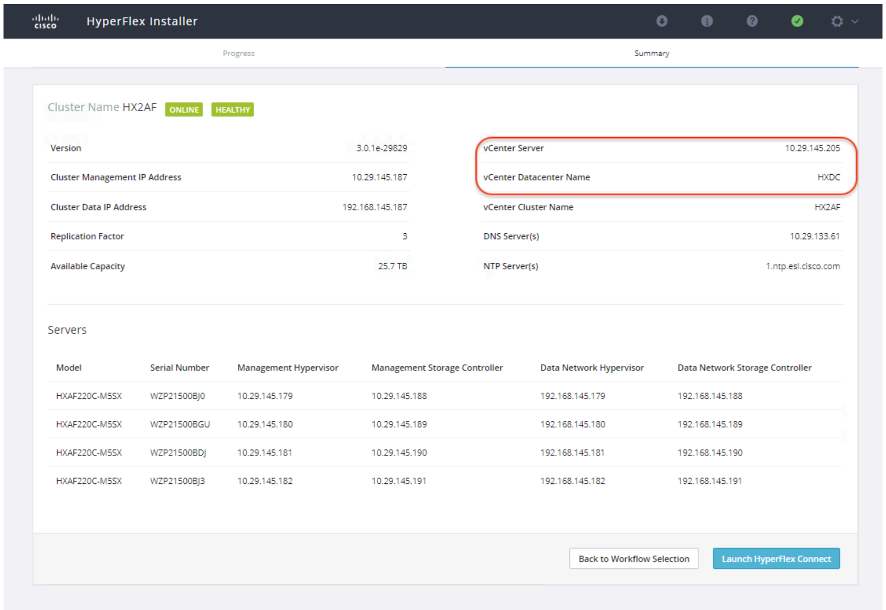
Here is an example of the command:

```
# stcli cluster reregister --vcenter-datacenter HXDC --vcenter-cluster HX2AF --vcenter-url
10.29.145.205 --vcenter-user administrator@vsphere.local
Register StorFS cluster with vCenter ...
Enter NEW vCenter Administrator password: *****
Cluster registration with new vCenter succeeded
```

9. Log in to vSphere Web Client and verify that the HX Data Platform plug-in appears in the extension list.



10. Refresh the Summary page of the Cisco HyperFlex installer. Verify that now the vCenter Server is specified.



Cluster Name HX2AF ONLINE HEALTHY

Version	3.0.1e-29829	vCenter Server	10.29.145.205
Cluster Management IP Address	10.29.145.187	vCenter Datacenter Name	HXDC
Cluster Data IP Address	192.168.145.187	vCenter Cluster Name	HX2AF
Replication Factor	3	DNS Server(s)	10.29.133.61
Available Capacity	25.7 TB	NTP Server(s)	1.ntp.esl.cisco.com

Servers

Model	Serial Number	Management Hypervisor	Management Storage Controller	Data Network Hypervisor	Data Network Storage Controller
HXAF220C-M5SX	WZP21500BJ0	10.29.145.179	10.29.145.188	192.168.145.179	192.168.145.188
HXAF220C-M5SX	WZP21500BGU	10.29.145.180	10.29.145.189	192.168.145.180	192.168.145.189
HXAF220C-M5SX	WZP21500BDJ	10.29.145.181	10.29.145.190	192.168.145.181	192.168.145.190
HXAF220C-M5SX	WZP21500BJ3	10.29.145.182	10.29.145.191	192.168.145.182	192.168.145.191

Performing Cisco HyperFlex post-installation configuration

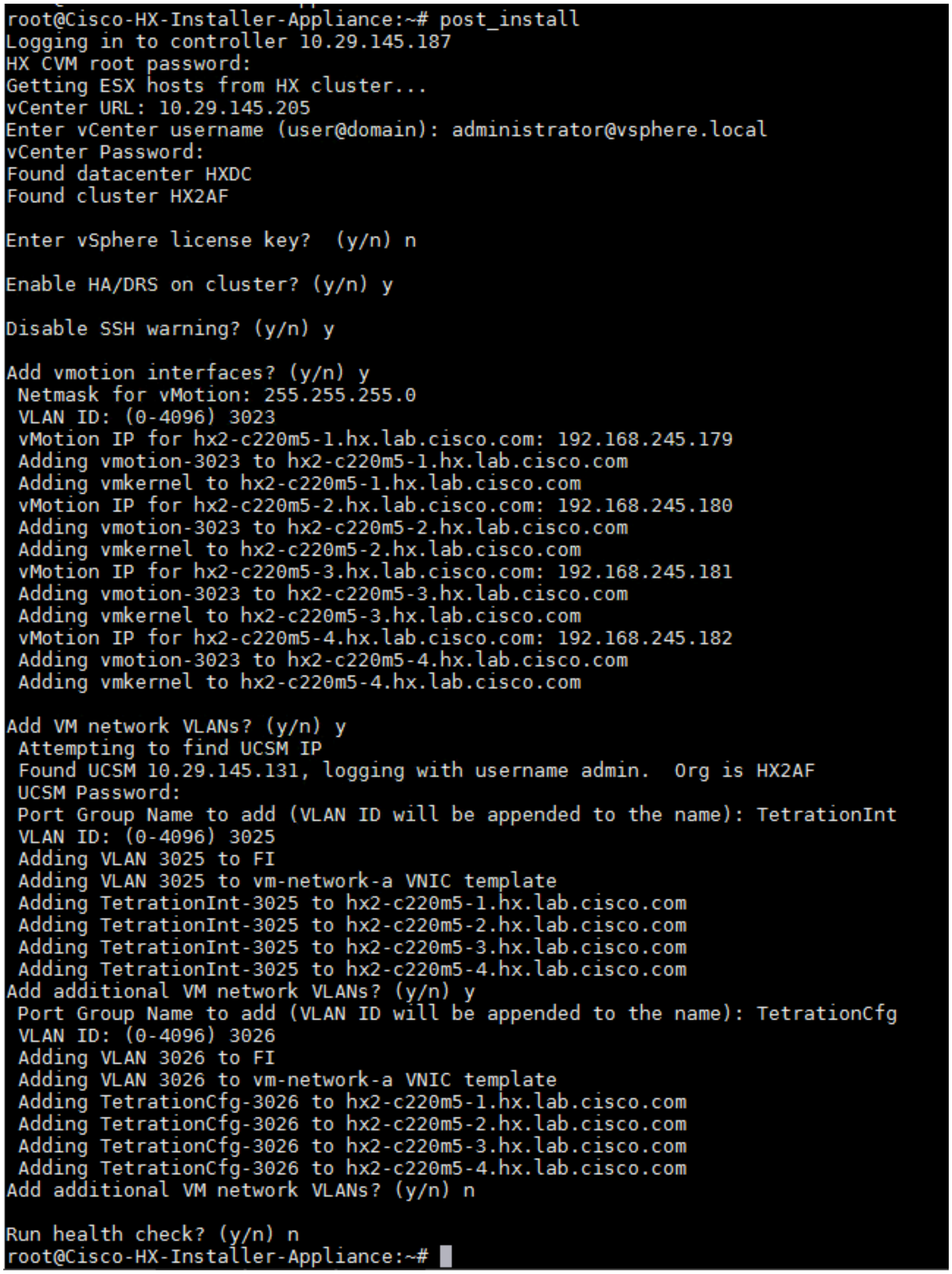
Use the following steps to run the **post_install** script from the Cisco HyperFlex Installer virtual machine to configure additional settings on the Cisco HyperFlex storage cluster.

1. Log in to the Cisco HyperFlex Installer virtual machine IP address using SSH and the root credentials.
2. Run the **post_install** script and follow the prompts.
3. The installer will already have the information from the just-completed Cisco HyperFlex installation, and the script will use this information. Enter the Cisco HyperFlex storage controller virtual machine root password for the Cisco HyperFlex cluster (use the name entered during the Cisco HyperFlex cluster installation), as well as the vCenter user name and password.
4. You can choose to enter the vSphere license here or complete this task later.
5. Enter **y** to enable HA and DRS if you have the appropriate licenses.
6. Enter **y** to disable the ESXi hosts' SSH warning.
7. Add the VMware vMotion VMkernel interfaces to each node by entering **y**. Enter the netmask, the vMotion VLAN ID, and the vMotion IP addresses for each of the hosts as prompted.
8. Enter **y** to add virtual machine VLANs to create two guest network port groups: one for Tetration Private Network and another for Tetration Configuration Network.

Note: The VLANs that will be used for Tetration-V installation must already be trunked to the Cisco UCS fabric interconnects from the northbound network by the upstream switches, and this configuration step must be performed manually prior to beginning the Cisco Tetration deployment.

9. If desired, enter **y** to run a health check on the cluster, or enter **n** to skip this step.

Here is an example of a completed configuration:



```
root@Cisco-HX-Installer-Appliance:~# post_install
Logging in to controller 10.29.145.187
HX CVM root password:
Getting ESX hosts from HX cluster...
vCenter URL: 10.29.145.205
Enter vCenter username (user@domain): administrator@vsphere.local
vCenter Password:
Found datacenter HXDC
Found cluster HX2AF

Enter vSphere license key?  (y/n) n

Enable HA/DRS on cluster? (y/n) y

Disable SSH warning? (y/n) y

Add vmotion interfaces? (y/n) y
 Netmask for vMotion: 255.255.255.0
 VLAN ID: (0-4096) 3023
 vMotion IP for hx2-c220m5-1.hx.lab.cisco.com: 192.168.245.179
 Adding vmotion-3023 to hx2-c220m5-1.hx.lab.cisco.com
 Adding vmkernel to hx2-c220m5-1.hx.lab.cisco.com
 vMotion IP for hx2-c220m5-2.hx.lab.cisco.com: 192.168.245.180
 Adding vmotion-3023 to hx2-c220m5-2.hx.lab.cisco.com
 Adding vmkernel to hx2-c220m5-2.hx.lab.cisco.com
 vMotion IP for hx2-c220m5-3.hx.lab.cisco.com: 192.168.245.181
 Adding vmotion-3023 to hx2-c220m5-3.hx.lab.cisco.com
 Adding vmkernel to hx2-c220m5-3.hx.lab.cisco.com
 vMotion IP for hx2-c220m5-4.hx.lab.cisco.com: 192.168.245.182
 Adding vmotion-3023 to hx2-c220m5-4.hx.lab.cisco.com
 Adding vmkernel to hx2-c220m5-4.hx.lab.cisco.com

Add VM network VLANs? (y/n) y
 Attempting to find UCSM IP
 Found UCSM 10.29.145.131, logging with username admin.  Org is HX2AF
 UCSM Password:
 Port Group Name to add (VLAN ID will be appended to the name): TetrationInt
 VLAN ID: (0-4096) 3025
 Adding VLAN 3025 to FI
 Adding VLAN 3025 to vm-network-a VNIC template
 Adding TetrationInt-3025 to hx2-c220m5-1.hx.lab.cisco.com
 Adding TetrationInt-3025 to hx2-c220m5-2.hx.lab.cisco.com
 Adding TetrationInt-3025 to hx2-c220m5-3.hx.lab.cisco.com
 Adding TetrationInt-3025 to hx2-c220m5-4.hx.lab.cisco.com
Add additional VM network VLANs? (y/n) y
 Port Group Name to add (VLAN ID will be appended to the name): TetrationCfg
 VLAN ID: (0-4096) 3026
 Adding VLAN 3026 to FI
 Adding VLAN 3026 to vm-network-a VNIC template
 Adding TetrationCfg-3026 to hx2-c220m5-1.hx.lab.cisco.com
 Adding TetrationCfg-3026 to hx2-c220m5-2.hx.lab.cisco.com
 Adding TetrationCfg-3026 to hx2-c220m5-3.hx.lab.cisco.com
 Adding TetrationCfg-3026 to hx2-c220m5-4.hx.lab.cisco.com
Add additional VM network VLANs? (y/n) n

Run health check? (y/n) n
root@Cisco-HX-Installer-Appliance:~# █
```

10. (Optional) Create DRS pin rules for the vCenter virtual machine if you have the appropriate licenses.

These steps place the vCenter virtual machine on a known host, making troubleshooting and manual restart easier. You may need to search for the vCenter virtual machine on all hosts to perform any manual steps, such as, bringing up the vCenter virtual machine after a full shutdown. See the VMware documentation for additional information.

a. Click cluster > Manage > Settings > Configuration > VM/Host Groups.

b. Click Add and select Type: VM group.

c. Click Add, select the vCenter virtual machine, click OK, and click OK again.

d. Click Add, select Type: Host group, add an ESXi host, click OK, and click OK again.

e. Click VM/Host Rules and select Type: Virtual Machines to Hosts.

f. Select the virtual machine group created earlier, select "Should run on hosts in group," select the host group created earlier, and enter the rule name. Then click OK.

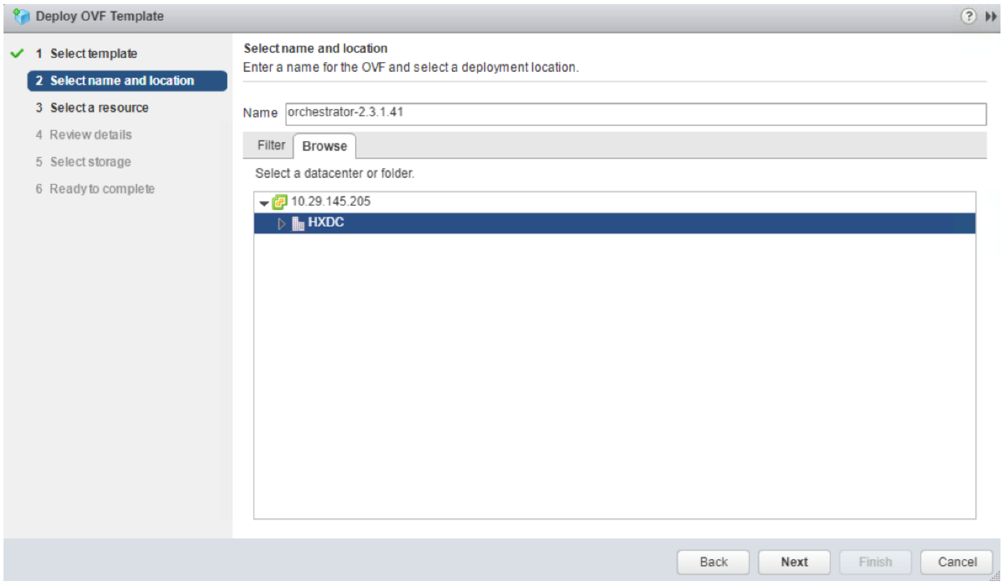
Cisco Tetration-V virtual appliance deployment

Follow the procedures here to deploy Tetration-V.

Installing the Cisco Tetration orchestrator virtual machine

Follow these steps to install the Cisco Tetration orchestrator virtual machine.

1. Download from the Cisco website the software-only virtual appliance OVA file for deploying Cisco Tetration in a VMware ESXi environment: for example, orchestrator-2.3.1.41.ova.
2. Log in to the vSphere vCenter web interface.
3. Right-click the Cisco HyperFlex cluster and choose Deploy OVF Template.
4. Enter the location of the downloaded OVF template file. Click Next.
5. Enter the name for the orchestrator virtual machine and choose the data center in which the virtual machine is deployed. Click Next.



Deploy OVF Template

1 Select template
2 Select name and location
3 Select a resource
4 Review details
5 Select storage
6 Ready to complete

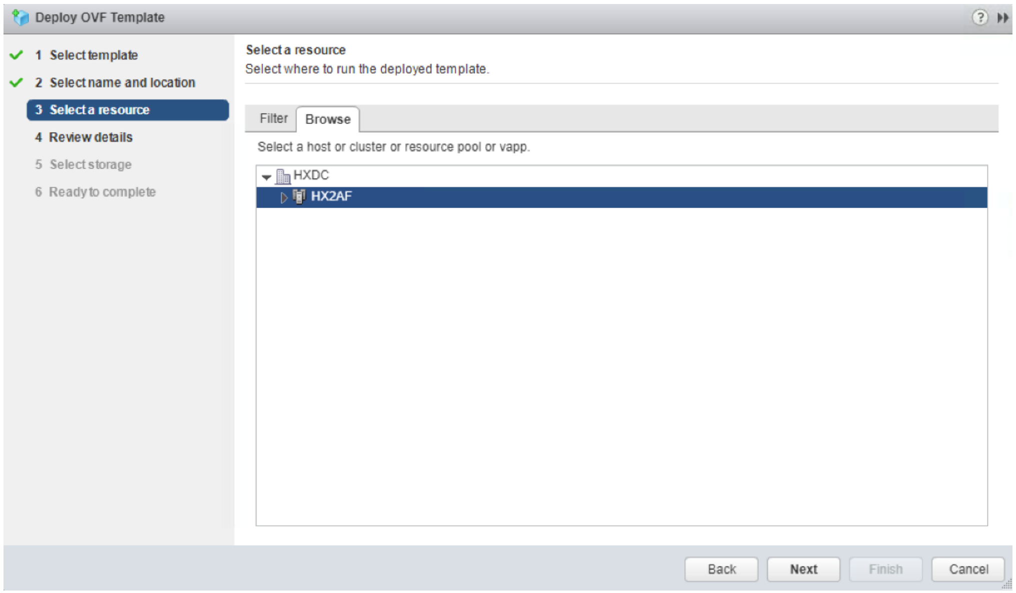
Select name and location
Enter a name for the OVF and select a deployment location.

Name: orchestrator-2.3.1.41

Select a datacenter or folder.

- 10.29.145.205
  - HXDC

6. Choose the Cisco HyperFlex cluster that is the intended target. Click Next.



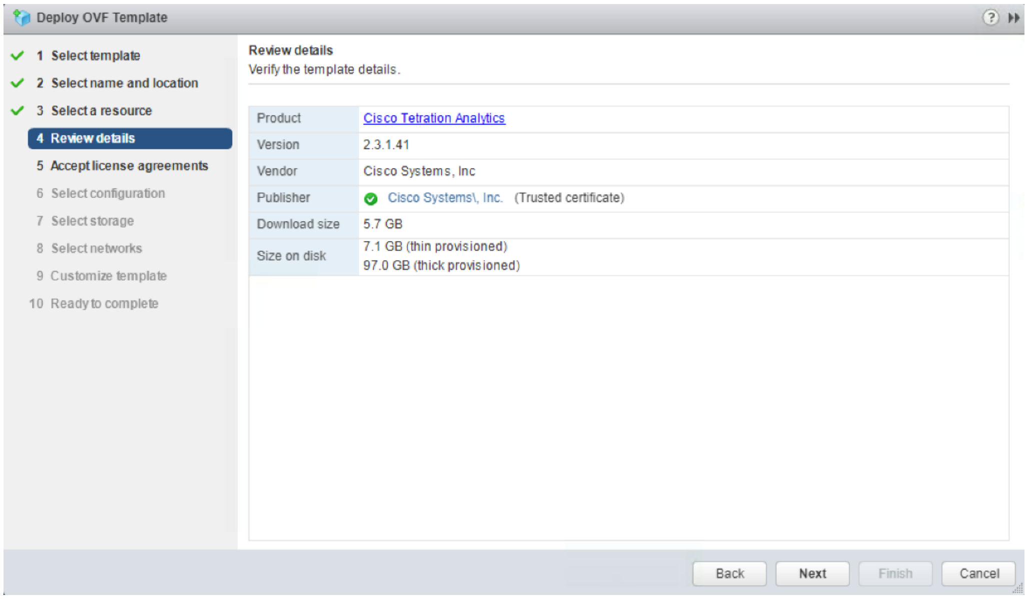
Select a resource

Select where to run the deployed template.

Select a host or cluster or resource pool or vapp.

- HXDC
  - HX2AF

7. Review the required resources. Click Next.

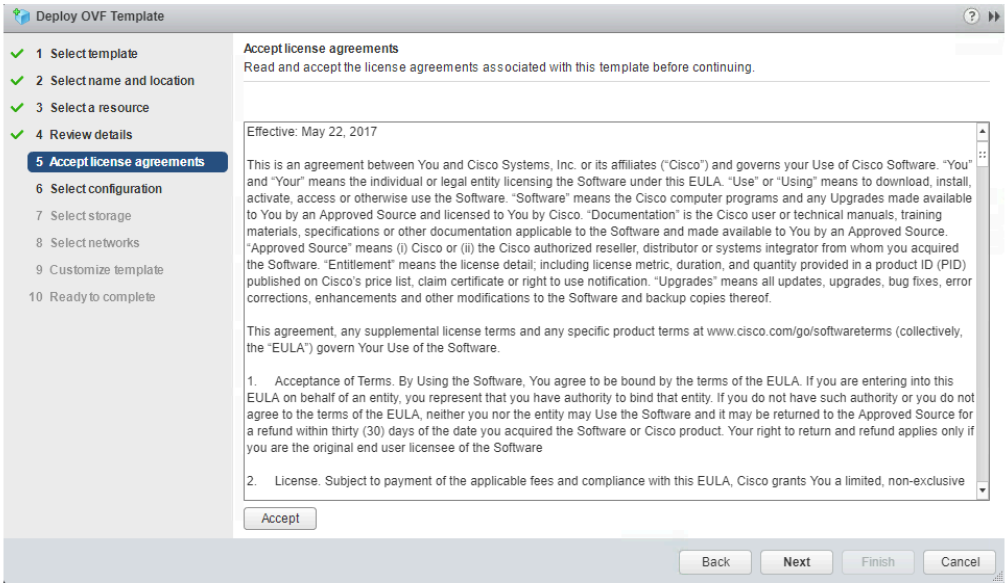


Review details

Verify the template details.

Product	Cisco Tetration Analytics
Version	2.3.1.41
Vendor	Cisco Systems, Inc
Publisher	✓ Cisco Systems\, Inc. (Trusted certificate)
Download size	5.7 GB
Size on disk	7.1 GB (thin provisioned) 97.0 GB (thick provisioned)

8. Review the license agreements and if you agree to the terms, click Accept. Then click Next.



Accept license agreements

Read and accept the license agreements associated with this template before continuing.

Effective: May 22, 2017

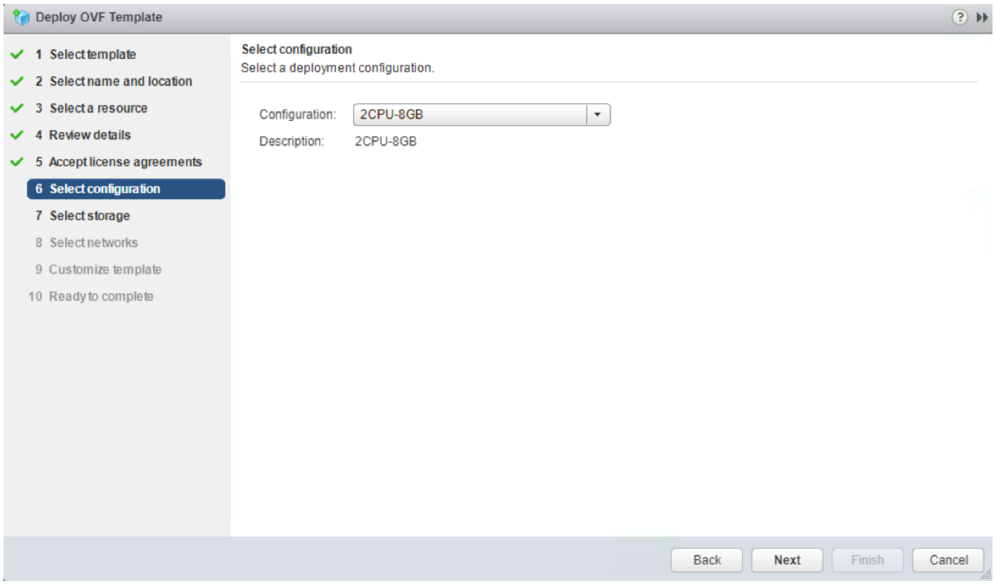
This is an agreement between You and Cisco Systems, Inc. or its affiliates ("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the individual or legal entity licensing the Software under this EULA. "Use" or "Using" means to download, install, activate, access or otherwise use the Software. "Software" means the Cisco computer programs and any Upgrades made available to You by an Approved Source and licensed to You by Cisco. "Documentation" is the Cisco user or technical manuals, training materials, specifications or other documentation applicable to the Software and made available to You by an Approved Source. "Approved Source" means (i) Cisco or (ii) the Cisco authorized reseller, distributor or systems integrator from whom you acquired the Software. "Entitlement" means the license detail; including license metric, duration, and quantity provided in a product ID (PID) published on Cisco's price list, claim certificate or right to use notification. "Upgrades" means all updates, upgrades, bug fixes, error corrections, enhancements and other modifications to the Software and backup copies thereof.

This agreement, any supplemental license terms and any specific product terms at www.cisco.com/go/softwareterms (collectively, the "EULA") govern Your Use of the Software.

1. Acceptance of Terms. By Using the Software, You agree to be bound by the terms of the EULA. If you are entering into this EULA on behalf of an entity, you represent that you have authority to bind that entity. If you do not have such authority or you do not agree to the terms of the EULA, neither you nor the entity may Use the Software and it may be returned to the Approved Source for a refund within thirty (30) days of the date you acquired the Software or Cisco product. Your right to return and refund applies only if you are the original end user licensee of the Software

2. License. Subject to payment of the applicable fees and compliance with this EULA, Cisco grants You a limited, non-exclusive

9. Use the default configuration profile (2CPU-8GB) and click Next.



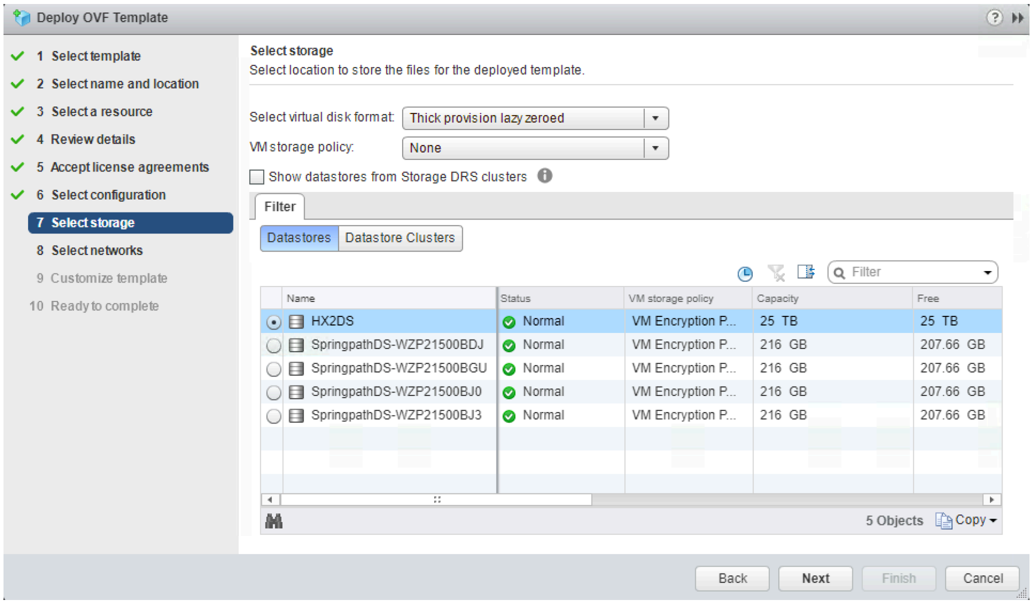
Select configuration

Select a deployment configuration.

Configuration: 2CPU-8GB

Description: 2CPU-8GB

10. Choose the Cisco HyperFlex data store that should be used for the deployment. Leave other options at the default settings. Click Next.



Deploy OVF Template

✓ 1 Select template
✓ 2 Select name and location
✓ 3 Select a resource
✓ 4 Review details
✓ 5 Accept license agreements
✓ 6 Select configuration
7 Select storage
8 Select networks
9 Customize template
10 Ready to complete

Select storage
Select location to store the files for the deployed template.

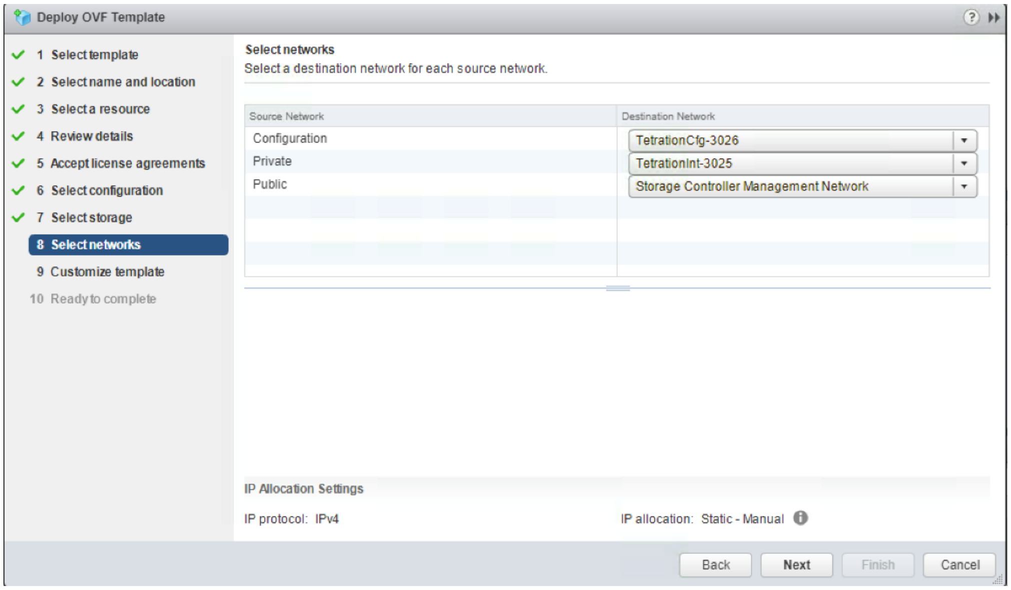
Select virtual disk format: Thick provision lazy zeroed
VM storage policy: None
□ Show datastores from Storage DRS clusters

Filter
Datastores | Datastore Clusters

	Name	Status	VM storage policy	Capacity	Free
●	HX2DS	Normal	VM Encryption P...	25 TB	25 TB
○	SpringpathDS-WZP21500BDJ	Normal	VM Encryption P...	216 GB	207.66 GB
○	SpringpathDS-WZP21500BGU	Normal	VM Encryption P...	216 GB	207.66 GB
○	SpringpathDS-WZP21500BJ0	Normal	VM Encryption P...	216 GB	207.66 GB
○	SpringpathDS-WZP21500BJ3	Normal	VM Encryption P...	216 GB	207.66 GB

5 Objects

11. Choose the appropriate network settings according to the Cisco HyperFlex network configuration and post-installation configuration. Click Next.



Deploy OVF Template

✓ 1 Select template
✓ 2 Select name and location
✓ 3 Select a resource
✓ 4 Review details
✓ 5 Accept license agreements
✓ 6 Select configuration
✓ 7 Select storage
8 Select networks
9 Customize template
10 Ready to complete

Select networks
Select a destination network for each source network.

Source Network	Destination Network
Configuration	TetrationCfg-3026
Private	TetrationInt-3025
Public	Storage Controller Management Network

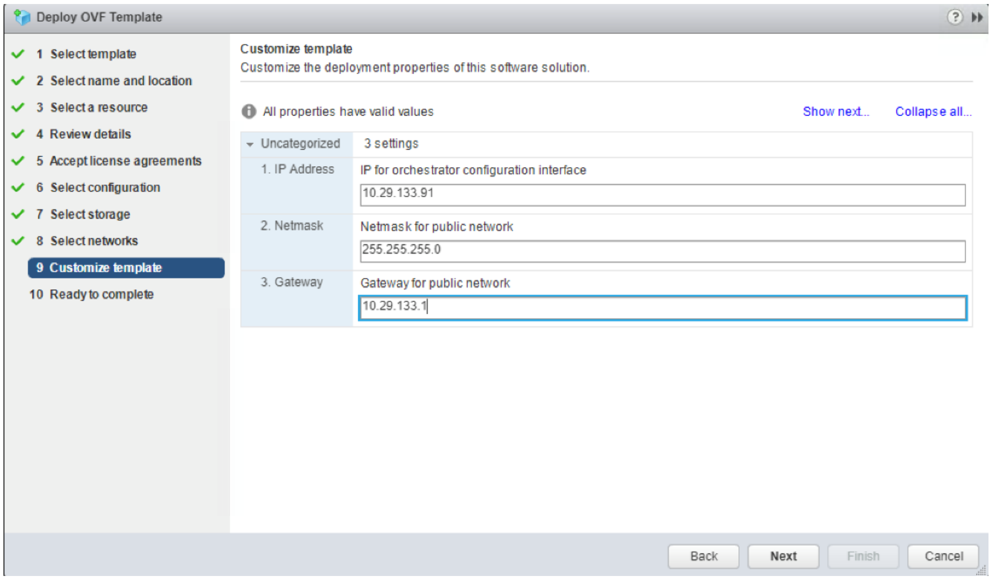
IP Allocation Settings
IP protocol: IPv4
IP allocation: Static - Manual

Table 5 shows the mapping applied for this document between the Tetration-V network and the Cisco HyperFlex network.

Table 5. Mapping between Cisco Tetration-V and Cisco HyperFlex networks

Tetration-V network	Cisco HyperFlex VLAN	Notes
Configuration	Cisco Tetration configuration VLAN on the guest virtual machine network	Additional Cisco HyperFlex guest virtual machine port group created in the post-installation configuration
Private	Cisco Tetration private VLAN on the guest virtual machine network	Additional Cisco HyperFlex guest virtual machine port group created in the post-installation configuration
Public	Cisco HyperFlex storage controller management VLAN	The network can be the same as the Cisco HyperFlex management network, or it can be different, depending on the local environment.

12. Enter the orchestrator's IP configuration. Click Next.



Customize template
Customize the deployment properties of this software solution.

All properties have valid values

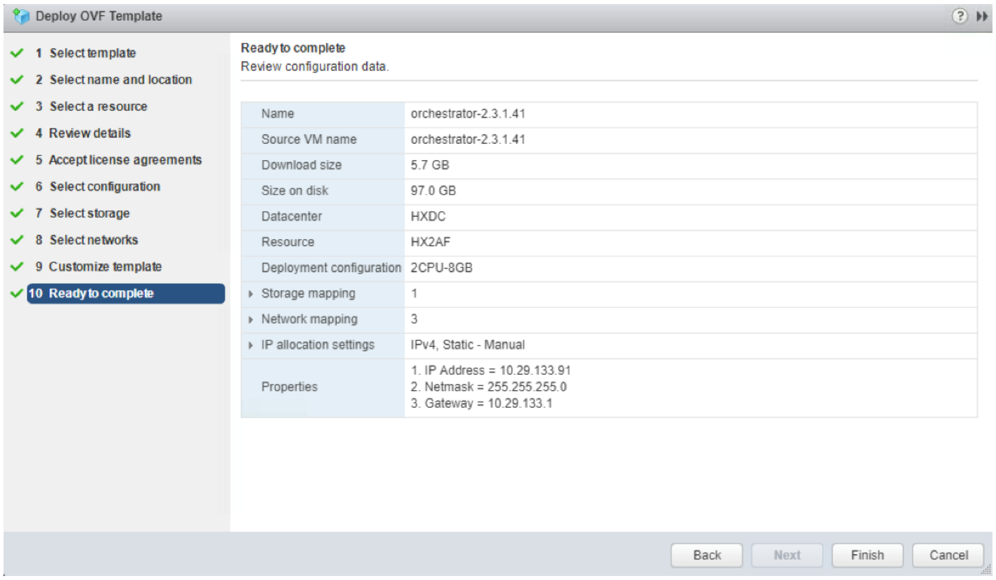
Uncategorized 3 settings

1. IP Address — IP for orchestrator configuration interface: 10.29.133.91

2. Netmask — Netmask for public network: 255.255.255.0

3. Gateway — Gateway for public network: 10.29.133.1

13. Review and confirm all your configuration parameters. Click Finish.



Ready to complete
Review configuration data.

Name	orchestrator-2.3.1.41
Source VM name	orchestrator-2.3.1.41
Download size	5.7 GB
Size on disk	97.0 GB
Datacenter	HXDC
Resource	HX2AF
Deployment configuration	2CPU-8GB
Storage mapping	1
Network mapping	3
IP allocation settings	IPv4, Static - Manual
Properties	1. IP Address = 10.29.133.91 2. Netmask = 255.255.255.0 3. Gateway = 10.29.133.1

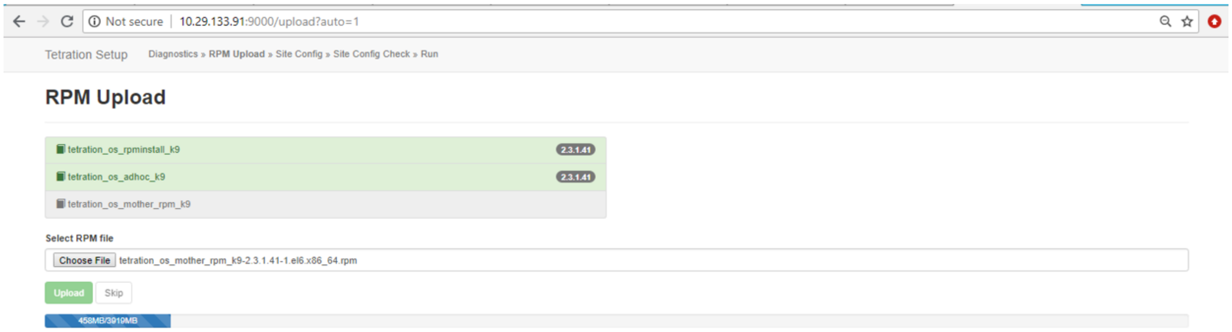
14. Wait a few minutes for the OVF deployment to be completed.
15. Go back to the vSphere web client and power on the orchestrator virtual machine.

You are now ready to deploy the full set of Cisco Tetration Analytics appliance files from the orchestrator virtual machine.

Configure Cisco Tetration-V virtual appliance

Follow these steps to configure Cisco Tetration-V.

1. Download the Cisco Tetration RPMs from the Cisco website. The following files are required:
   - rpminstall
   - adhoc
   - mother
2. Open a new browser tab, enter the IP address of the orchestrator virtual machine and add port 9000 after the IP address. For example, enter http://10.29.133.91:9000. Click Enter to open the Tetration Setup GUI.
3. In the Tetration Setup GUI, choose and upload the RPM files one by one in the following order:
   - rpminstall
   - adhoc
   - mother


Not secure
Tetration Setup
Diagnostics » RPM Upload » Site Config » Site Config Check » Run
Upload
Skip

10.29.133.91:9000/upload?auto=1

RPM Upload

tetration_os_rpminstall_k9 2.3.1.41

tetration_os_adhoc_k9 2.3.1.41

tetration_os_mother_rpm_k9

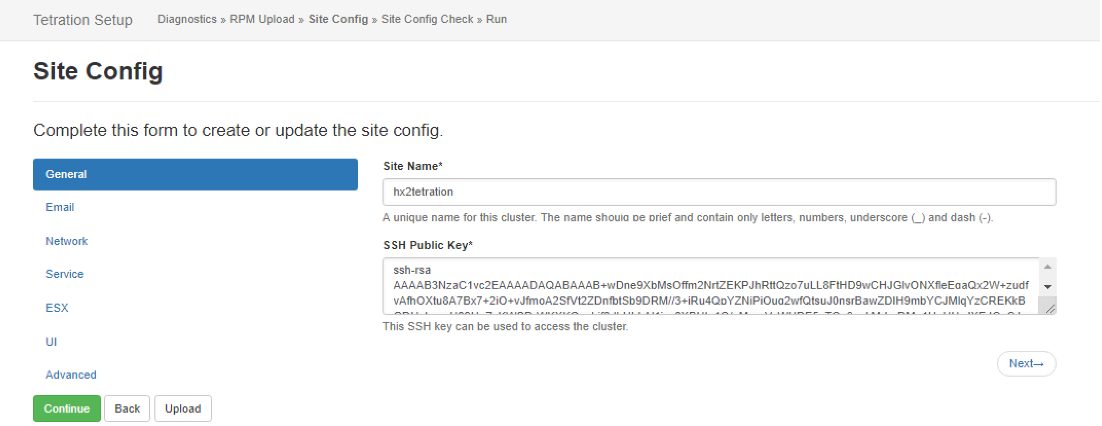
Select RPM file

Choose File tetration_os_mother_rpm_k9-2.3.1.41-1.el6.x86_64.rpm

458MB/3919MB

The Cisco Tetration installation procedure starts automatically after the files are uploaded.

4. For Site Configuration, on the General page, enter the site name and SSH public key (you can generate the key by using the **ssh-keygen** command). Click Continue.



Site Config

Complete this form to create or update the site config.

Site Name*

hx2tetration

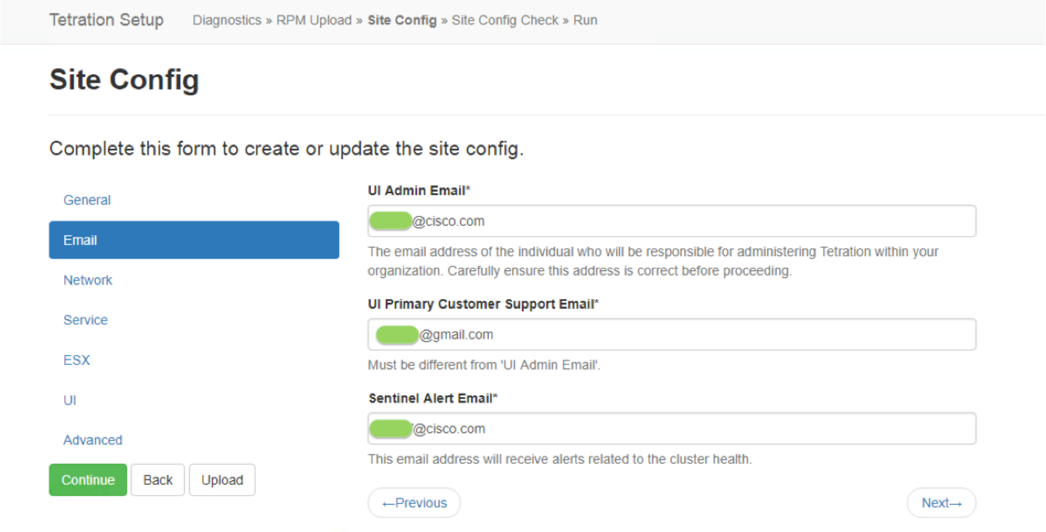
A unique name for this cluster. The name should be brief and contain only letters, numbers, underscore (_) and dash (-).

SSH Public Key*

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAB+wDne9XbMsOffm2NrtZEKPJhRttQzo7uLL8FtHD9wCHJGlvONXfleEqaQx2W+zudf
vAfhOXtu8A7Bx7+2iO+vJfmoA2SfVt2ZDnfbtSb9DRM//3+iRu4QpYZNiPiOuq2wfQtsuJ0nsrBawZDIH9mbYCJMlqYzCREKkB
```

This SSH key can be used to access the cluster.

5. On the Email page, provide the required email addresses and click Continue. Three email accounts are needed:
    - User interface administrator email account
    - User interface primary customer support email account
    - Sentinel alert email account



Site Config

Complete this form to create or update the site config.

UI Admin Email*

[redacted]@cisco.com

The email address of the individual who will be responsible for administering Tetration within your organization. Carefully ensure this address is correct before proceeding.

UI Primary Customer Support Email*

[redacted]@gmail.com

Must be different from 'UI Admin Email'.

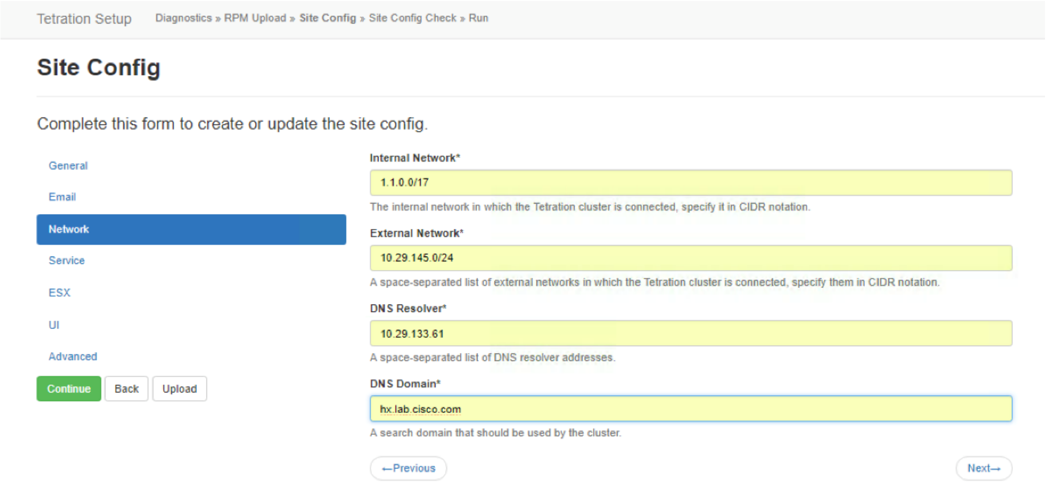
Sentinel Alert Email*

[redacted]@cisco.com

This email address will receive alerts related to the cluster health.

Click Continue.

6. On the Network page, enter the internal and external network settings, DNS IP address, and domain information. For the internal network configuration, you can use the address that is in the orchestrator deployment output. Click Continue.



Site Config

Complete this form to create or update the site config.

Internal Network*

1.1.0.0/17

The internal network in which the Tetration cluster is connected, specify it in CIDR notation.

External Network*

10.29.145.0/24

A space-separated list of external networks in which the Tetration cluster is connected, specify them in CIDR notation.

DNS Resolver*

10.29.133.61

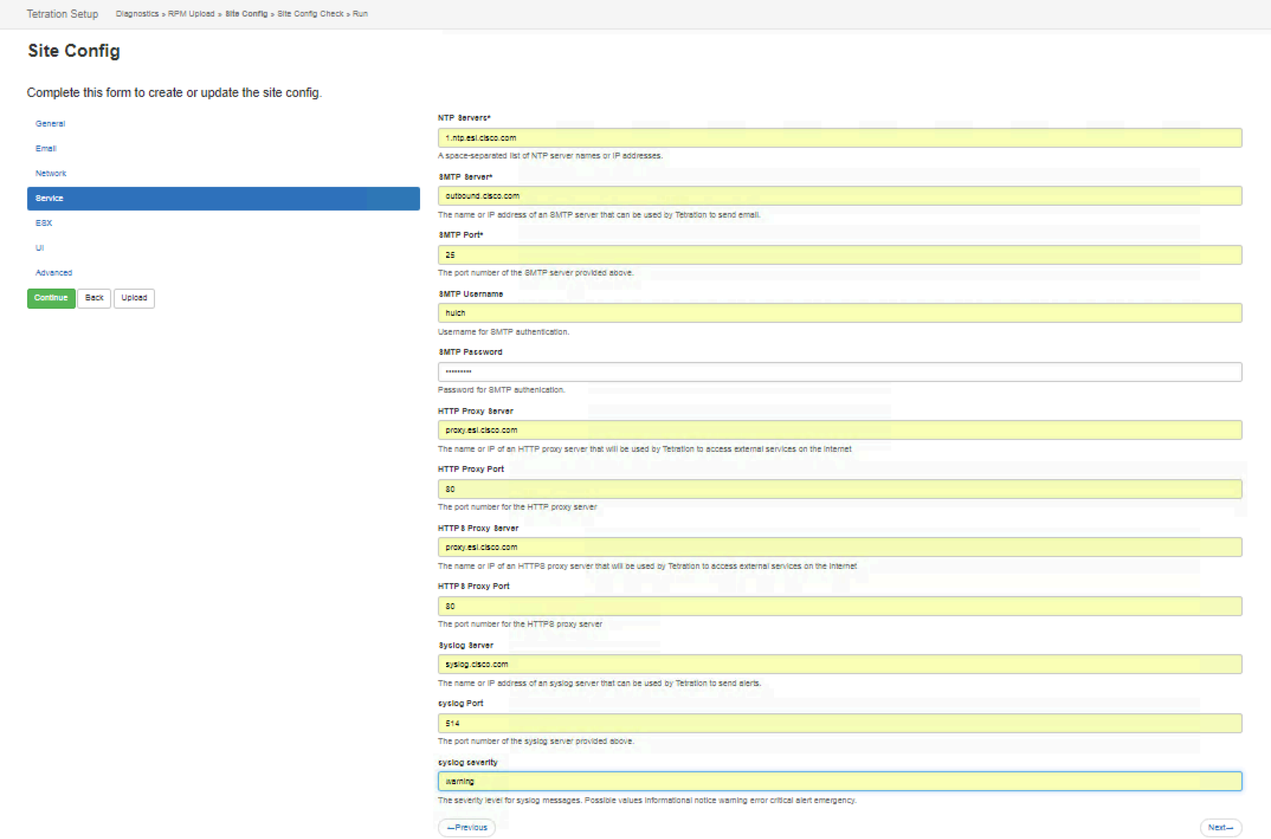
A space-separated list of DNS resolver addresses.

DNS Domain*

hx.lab.cisco.com

A search domain that should be used by the cluster.

7. On the Service page, enter the settings in your local network for the NTP, Simple Mail Transfer Protocol (SMTP), HTTP proxy, and syslog services. Click Continue.



Tetration Setup
Diagnostics » RPM Upload » Site Config » Site Config Check » Run

Site Config

Complete this form to create or update the site config.

NTP Servers*
1.ntp.esl.cisco.com
A space-separated list of NTP server names or IP addresses.

SMTP Server*
outbound.cisco.com
The name or IP address of an SMTP server that can be used by Tetration to send email.

SMTP Port*
25
The port number of the SMTP server provided above.

SMTP Username
hulch
Username for SMTP authentication.

SMTP Password
••••••••••
Password for SMTP authenication.

HTTP Proxy Server
proxy.esl.cisco.com
The name or IP of an HTTP proxy server that will be used by Tetration to access external services on the Internet

HTTP Proxy Port
80
The port number for the HTTP proxy server

HTTPS Proxy Server
proxy.esl.cisco.com
The name or IP of an HTTPS proxy server that will be used by Tetration to access external services on the Internet

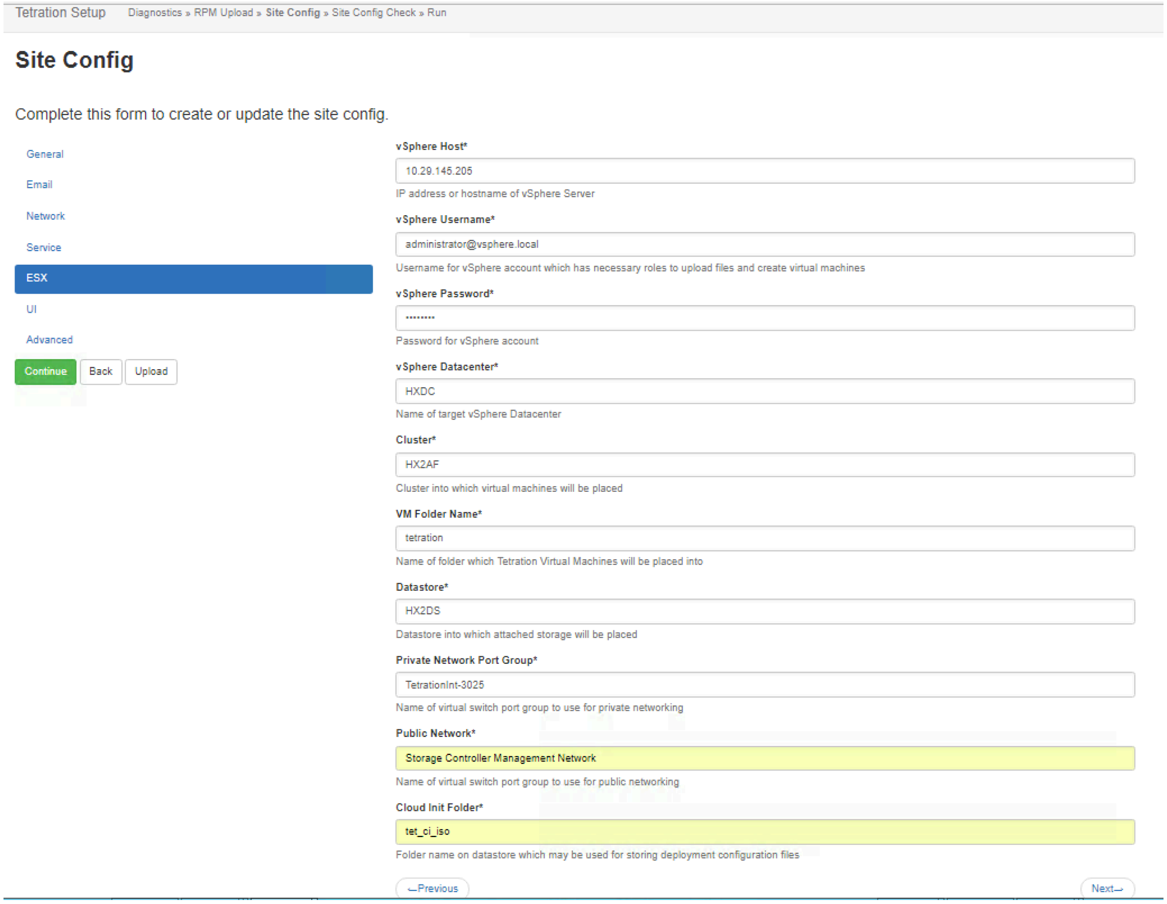
HTTPS Proxy Port
80
The port number for the HTTPS proxy server

Syslog Server
syslog.cisco.com
The name or IP address of an syslog server that can be used by Tetration to send alerts.

syslog Port
514
The port number of the syslog server provided above.

syslog severity
warning
The severity level for syslog messages. Possible values informational notice warning error critical alert emergency.

8. On the ESX page, enter the vSphere vCenter access information and Cisco HyperFlex cluster name and Cisco HyperFlex data store for the Cisco Tetration virtual machine deployment. Enter the port group names for the Cisco Tetration private and public networks. Click Continue.



Site Config

Complete this form to create or update the site config.

vSphere Host*
10.29.145.205
IP address or hostname of vSphere Server

vSphere Username*
administrator@vsphere.local
Username for vSphere account which has necessary roles to upload files and create virtual machines

vSphere Password*
••••••••
Password for vSphere account

vSphere Datacenter*
HXDC
Name of target vSphere Datacenter

Cluster*
HX2AF
Cluster into which virtual machines will be placed

VM Folder Name*
tetration
Name of folder which Tetration Virtual Machines will be placed into

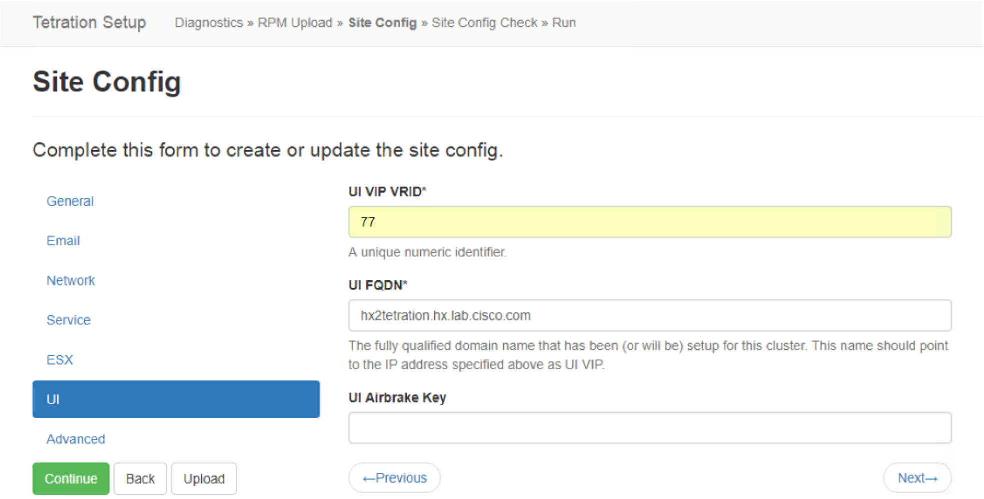
Datastore*
HX2DS
Datastore into which attached storage will be placed

Private Network Port Group*
TetrationInt-3025
Name of virtual switch port group to use for private networking

Public Network*
Storage Controller Management Network
Name of virtual switch port group to use for public networking

Cloud Init Folder*
tet_ci_iso
Folder name on datastore which may be used for storing deployment configuration files

9. On the UI page, enter a unique number for the virtual router identifier (VRID) and the fully qualified domain name (FQDN) for the appliance. Leave the airbrake key blank. Click Continue.



Site Config

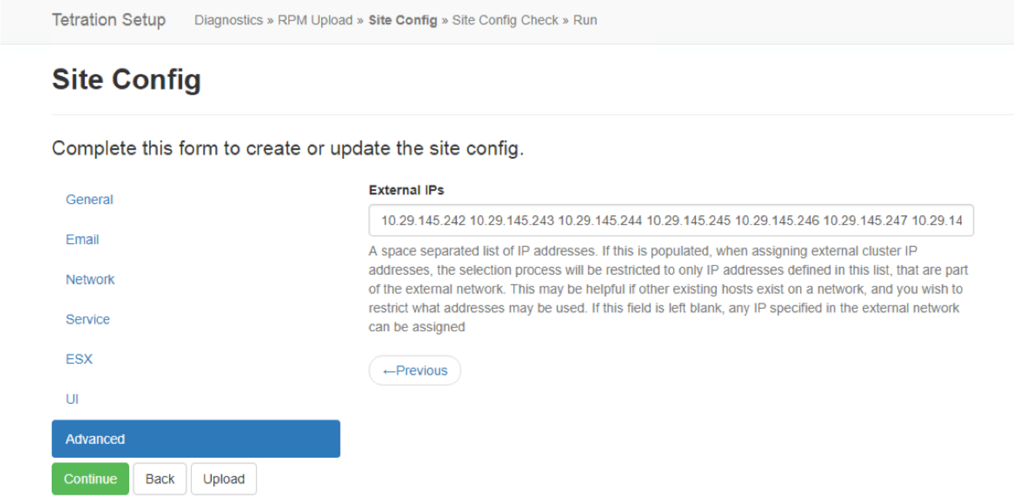
Complete this form to create or update the site config.

UI VIP VRID*
77
A unique numeric identifier.

UI FQDN*
hx2tetration.hx.lab.cisco.com
The fully qualified domain name that has been (or will be) setup for this cluster. This name should point to the IP address specified above as UI VIP.

UI Airbrake Key

10. On the Advanced page, enter the external IP addresses (eight IP addresses are required) that are available to this Cisco Tetration virtual appliance.



Tetration Setup
Diagnostics » RPM Upload » **Site Config** » Site Config Check » Run

Site Config

Complete this form to create or update the site config.

General
Email
Network
Service
ESX
UI
Advanced

External IPs

10.29.145.242 10.29.145.243 10.29.145.244 10.29.145.245 10.29.145.246 10.29.145.247 10.29.14

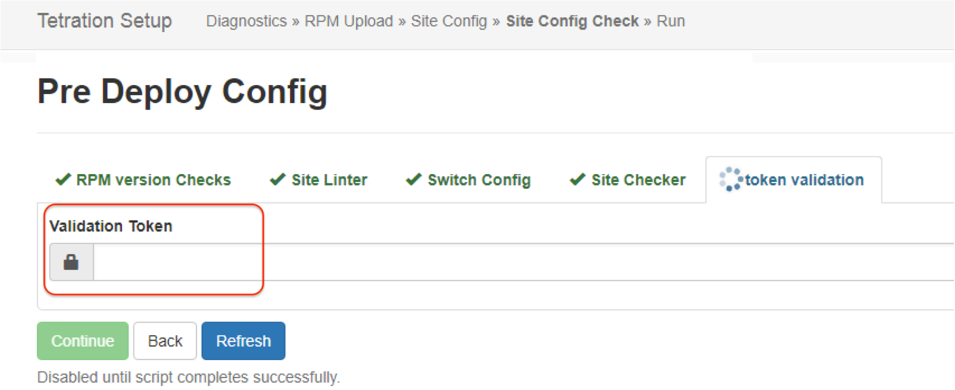
A space separated list of IP addresses. If this is populated, when assigning external cluster IP addresses, the selection process will be restricted to only IP addresses defined in this list, that are part of the external network. This may be helpful if other existing hosts exist on a network, and you wish to restrict what addresses may be used. If this field is left blank, any IP specified in the external network can be assigned

Click Continue to start the deployment process.

Deploying the Cisco Tetration-V virtual appliance

At the Pre Deploy Config stage of the deployment, you will be asked for a validation token to continue.

1. View the Pre Deploy Config page.



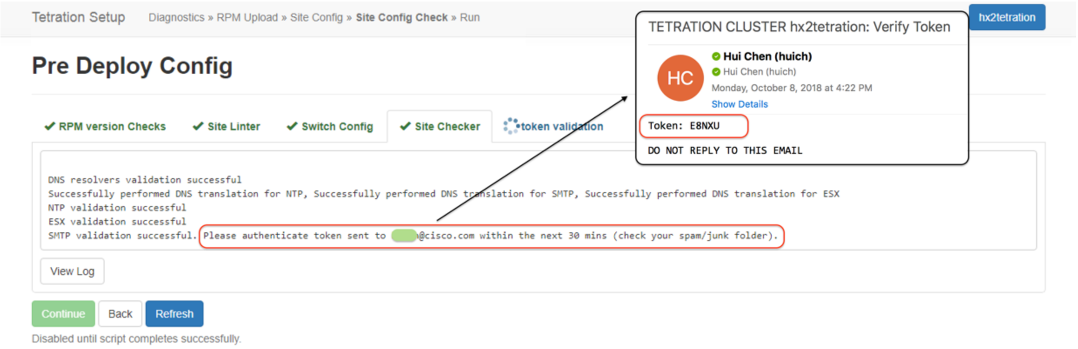
Tetration Setup
Diagnostics » RPM Upload » Site Config » **Site Config Check** » Run

Pre Deploy Config

Validation Token

Disabled until script completes successfully.

2. The token was sent to the administration email address you provided during the configuration. You can click the Site Checker tab to see the email address that was used to send this token.



Tetration Setup
Diagnostics » RPM Upload » Site Config » **Site Config Check** » Run
hx2tetration

Pre Deploy Config

```
DNS resolvers validation successful
Successfully performed DNS translation for NTP, Successfully performed DNS translation for SMTP, Successfully performed DNS translation for ESX
NTP validation successful
ESX validation successful
SMTP validation successful. Please authenticate token sent to [redacted]@cisco.com within the next 30 mins (check your spam/junk folder).
```

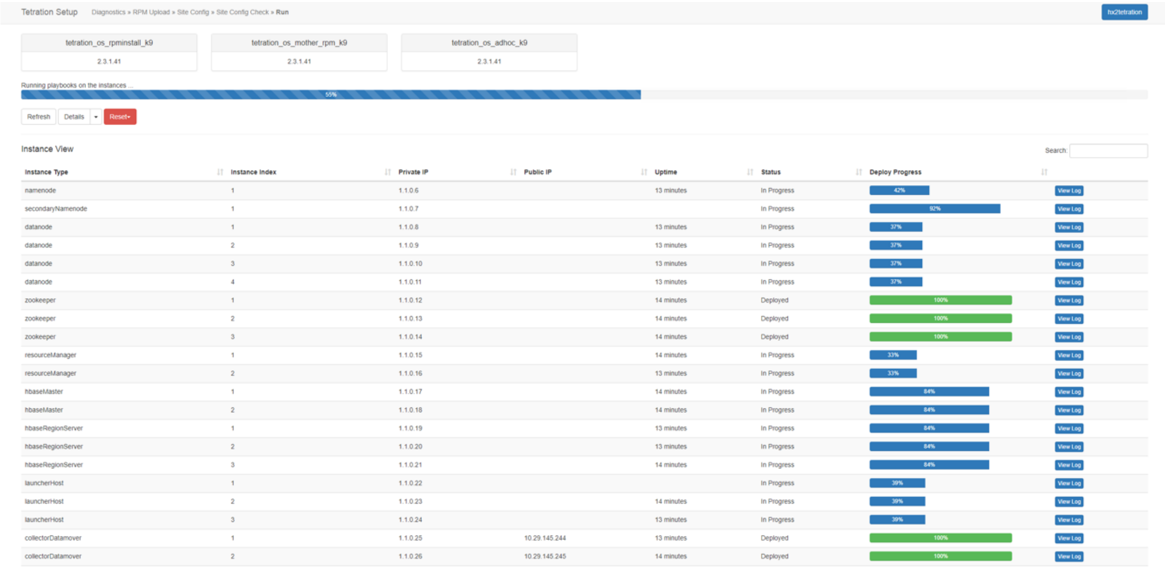
TETRATION CLUSTER hx2tetration: Verify Token

Hui Chen (huich)
Hui Chen (huich)
Monday, October 8, 2018 at 4:22 PM
Show Details

```
Token: E8NXU

DO NOT REPLY TO THIS EMAIL
```

Disabled until script completes successfully.

3. Enter the received token and click Continue. The deployment process will now start.


Tetration Setup
Diagnostics » RPM Upload » Site Config » Site Config Check » Run
hx2tetration
55%
Refresh
Details
Reset
Search:
View Log

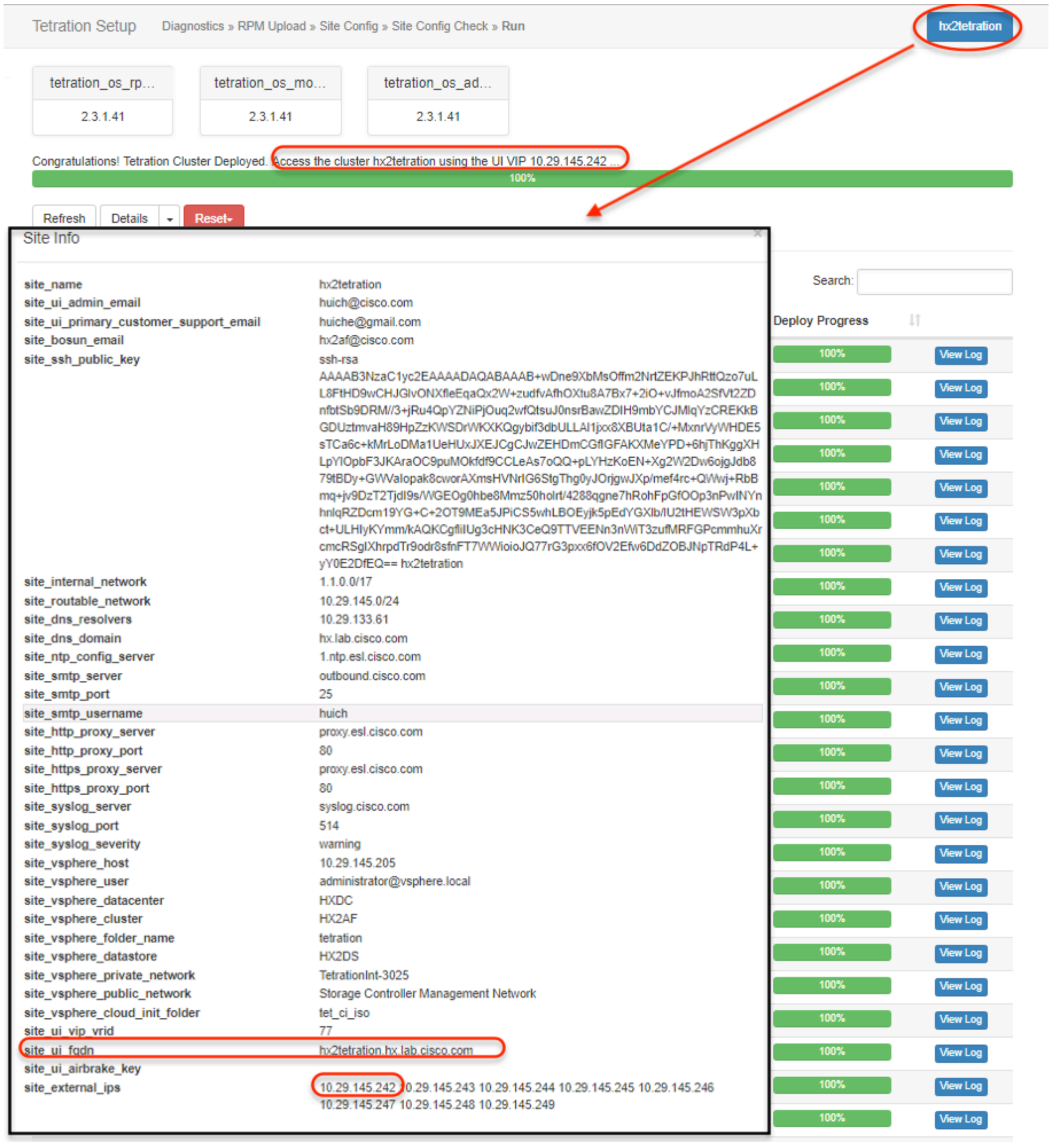
tetration_os_rpminstall_k9	tetration_os_mother_rpm_k9	tetration_os_adhoc_k9
2.3.1.41	2.3.1.41	2.3.1.41

Running playbooks on the instances ...

Instance View

Instance Type	Instance Index	Private IP	Public IP	Uptime	Status	Deploy Progress
namenode	1	1.1.0.6		13 minutes	In Progress	42%
secondaryNamenode	1	1.1.0.7			In Progress	92%
datanode	1	1.1.0.8		13 minutes	In Progress	37%
datanode	2	1.1.0.9		13 minutes	In Progress	37%
datanode	3	1.1.0.10		13 minutes	In Progress	37%
datanode	4	1.1.0.11		13 minutes	In Progress	37%
zookeeper	1	1.1.0.12		14 minutes	Deployed	100%
zookeeper	2	1.1.0.13		14 minutes	Deployed	100%
zookeeper	3	1.1.0.14		14 minutes	Deployed	100%
resourceManager	1	1.1.0.15		14 minutes	In Progress	33%
resourceManager	2	1.1.0.16		13 minutes	In Progress	33%
hbaseMaster	1	1.1.0.17		14 minutes	In Progress	84%
hbaseMaster	2	1.1.0.18		14 minutes	In Progress	84%
hbaseRegionServer	1	1.1.0.19		13 minutes	In Progress	84%
hbaseRegionServer	2	1.1.0.20		13 minutes	In Progress	84%
hbaseRegionServer	3	1.1.0.21		14 minutes	In Progress	84%
launcherHost	1	1.1.0.22			In Progress	39%
launcherHost	2	1.1.0.23		14 minutes	In Progress	39%
launcherHost	3	1.1.0.24		13 minutes	In Progress	39%
collectorDatamover	1	1.1.0.25	10.29.145.244	13 minutes	Deployed	100%
collectorDatamover	2	1.1.0.26	10.29.145.245	14 minutes	Deployed	100%

4. Deployment takes approximately 1.5 hours to complete. To review your site information, click the appliance name at the top-right corner.



Congratulations! Tetration Cluster Deployed. Access the cluster hx2tetration using the UI VIP 10.29.145.242 ...

Site Info

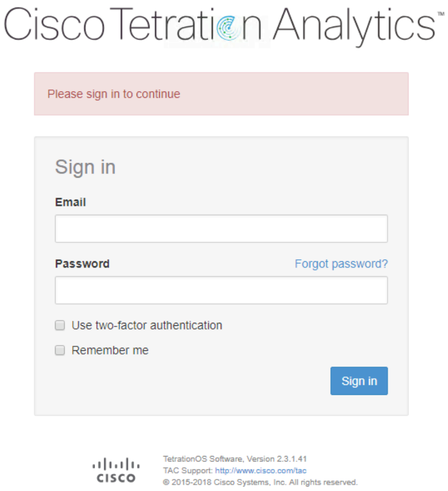
site_name	hx2tetration
site_ui_admin_email	huich@cisco.com
site_ui_primary_customer_support_email	huiche@gmail.com
site_bosun_email	hx2af@cisco.com
site_ssh_public_key	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAB+wDne9XbMsOffm2NrtZEKPJhRttQzo7uL L8FtHD9wCHJGlvONXfleEqaQx2W+zudfvAfhOXtu8A7Bx7+2iO+vJfmoA2SfVt2ZD nfbtSb9DRM//3+jRu4QpYZNiPjOuq2wfQtsuJ0nsrBawZDIH9mbYCJMlqYzCREKkB GDUztmvaH89HpZzKWSDrWKXKQgybif3dbULLAl1jxx8XBUta1C/+MxnrVyWHDE5 sTCa6c+kMrLoDMa1UeHUxJXEJCgCJwZEHDmCGflGFAKXMeYPD+6hjThKggXH LpYlOpbF3JKAraOC9puMOkfdf9CCLeAs7oQQ+pLYHzKoEN+Xg2W2Dw6ojgJdb8 79tBDy+GWValopak8cworAXmsHVNrlG6StgThg0yJOrjgwJXp/mef4rc+QWwj+RbB mq+jv9DzT2Tjdl9s/WGEOg0hbe8Mmz50holrt/4288qgne7hRohFpGfOOp3nPwINYn hnlqRZDcm19YG+C+2OT9MEa5JPiCS5whLBOEyjk5pEdYGXlb/IU2tHEWSW3pXb ct+ULHlyKYmm/kAQKCgfliIUg3cHNK3CeQ9TTVEENn3nWiT3zufMRFGPcmmhuXr cmcRSglXhrpdTr9odr8sfnFT7WWioioJQ77rG3pxx6fOV2Efw6DdZOBJNpTRdP4L+ yY0E2DfEQ== hx2tetration
site_internal_network	1.1.0.0/17
site_routable_network	10.29.145.0/24
site_dns_resolvers	10.29.133.61
site_dns_domain	hx.lab.cisco.com
site_ntp_config_server	1.ntp.esl.cisco.com
site_smtp_server	outbound.cisco.com
site_smtp_port	25
site_smtp_username	huich
site_http_proxy_server	proxy.esl.cisco.com
site_http_proxy_port	80
site_https_proxy_server	proxy.esl.cisco.com
site_https_proxy_port	80
site_syslog_server	syslog.cisco.com
site_syslog_port	514
site_syslog_severity	warning
site_vsphere_host	10.29.145.205
site_vsphere_user	administrator@vsphere.local
site_vsphere_datacenter	HXDC
site_vsphere_cluster	HX2AF
site_vsphere_folder_name	tetration
site_vsphere_datastore	HX2DS
site_vsphere_private_network	TetrationInt-3025
site_vsphere_public_network	Storage Controller Management Network
site_vsphere_cloud_init_folder	tet_ci_iso
site_ui_vip_vrid	77
site_ui_fqdn	hx2tetration.hx.lab.cisco.com
site_ui_airbrake_key	
site_external_ips	10.29.145.242 10.29.145.243 10.29.145.244 10.29.145.245 10.29.145.246 10.29.145.247 10.29.145.248 10.29.145.249

5. After the deployment progress has reached 100 percent, note the virtual IP address that is shown in the status line, which is the first available IP address that was provided to the installer. You can also use the user interface FQDN to access the Cisco Tetration Analytics Dashboard webpage.
6. The last step of the deployment process is to disable external access to the Tetration-V installer:
   a. In the vSphere web client, right-click the orchestrator-1 VM and choose Edit Settings.
   b. Click the Virtual Hardware tab.
   c. For Network Adapter 3, remove the checkmark from the Connected box.
   d. Click OK to apply the changes.

Verifying the installation

Now validate the installation.

1. Open your browser and point it to the user interface FQDN that you obtained in the site information to access the Cisco Tetration Analytics Dashboard webpage.
2. On the "Sign in" page, click Forgot Password?



Cisco Tetration Analytics™

Please sign in to continue

Sign in

Email

Password | Forgot password?

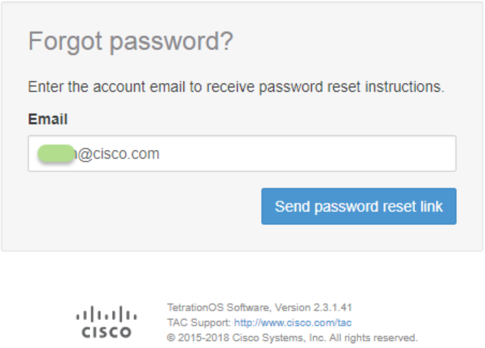
□ Use two-factor authentication

□ Remember me

Sign in

TetrationOS Software, Version 2.3.1.41
TAC Support: http://www.cisco.com/tac
© 2015-2018 Cisco Systems, Inc. All rights reserved.

3. Enter the email address that you entered for the site administrator and click "Send Password reset link."



Forgot password?

Enter the account email to receive password reset instructions.

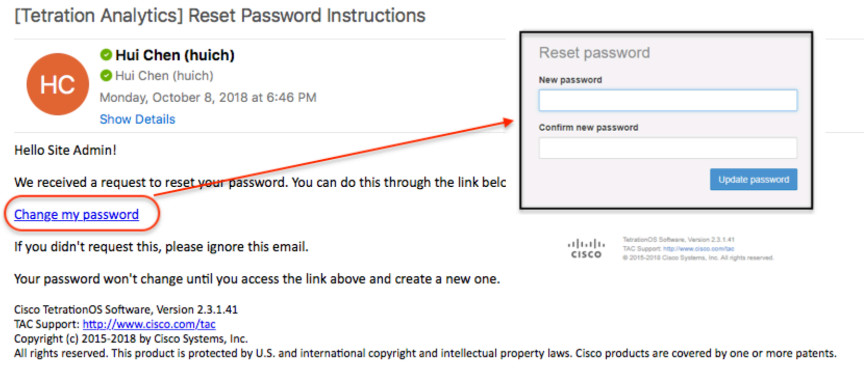
Email

[redacted]@cisco.com

Send password reset link

TetrationOS Software, Version 2.3.1.41
TAC Support: http://www.cisco.com/tac
© 2015-2018 Cisco Systems, Inc. All rights reserved.

4. Check your inbox for the email message and follow the included instructions to reset the password for the Cisco Tetration administrator.



[Tetration Analytics] Reset Password Instructions

HC Hui Chen (huich)
Hui Chen (huich)
Monday, October 8, 2018 at 6:46 PM
Show Details

Hello Site Admin!

We received a request to reset your password. You can do this through the link belc

Change my password

If you didn't request this, please ignore this email.

Your password won't change until you access the link above and create a new one.

Cisco TetrationOS Software, Version 2.3.1.41
TAC Support: http://www.cisco.com/tac
Copyright (c) 2015-2018 by Cisco Systems, Inc.
All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Cisco products are covered by one or more patents.

Reset password

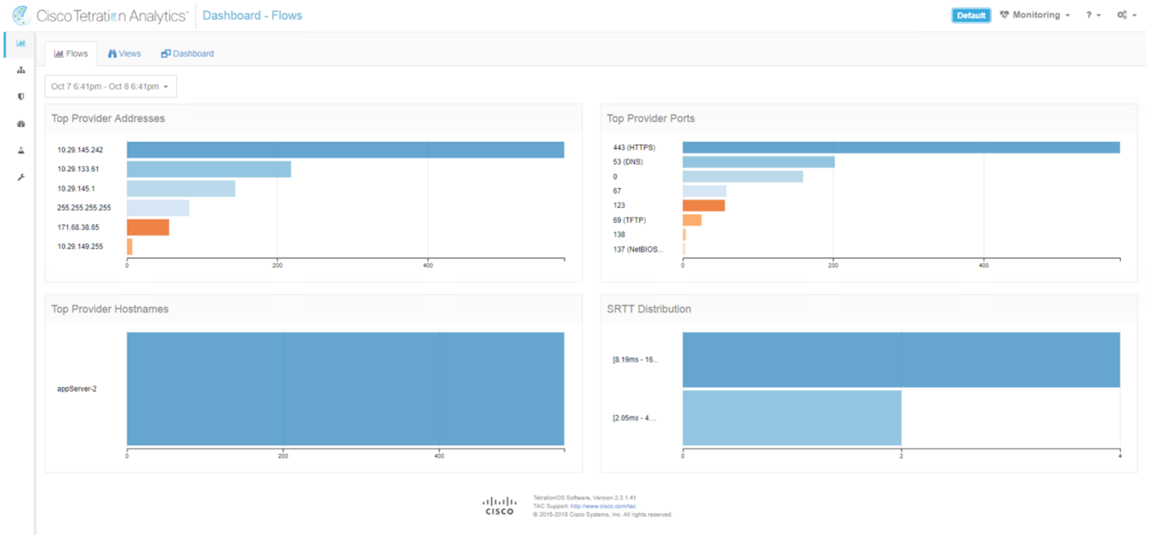
New password

Confirm new password

Update password

TetrationOS Software, Version 2.3.1.41
TAC Support: http://www.cisco.com/tac
© 2015-2018 Cisco Systems, Inc. All rights reserved.

5. Sign in to the Cisco Tetration Analytics Dashboard webpage with the new password. You should be taken to the dashboard of the newly installed Cisco Tetration virtual appliance.



Upgrading the Cisco Tetration-V virtual appliance

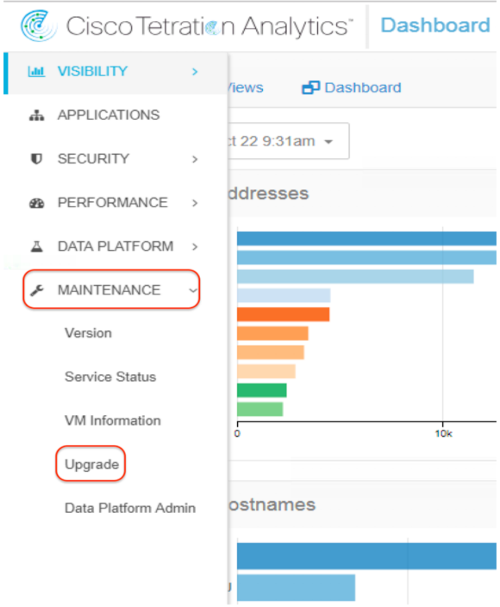
Before you begin the upgrade process, check the Cisco Tetration Analytics Upgrade Guide to see the supported upgrade paths and upgrade the patches in the specified order. You cannot skip any releases, unless otherwise specified.

Also download the desired RPM file from the Cisco website: for example, tetration_os_patch_k9-2.3.1.50-1.noarch.rpm.

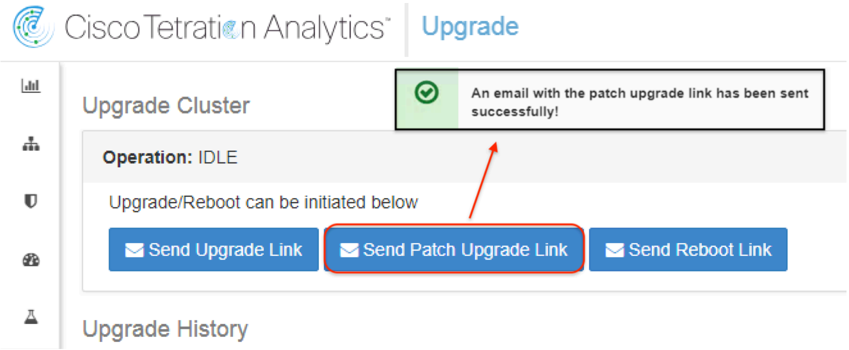
Note: Do not upgrade if any nodes are currently in a decommissioned state or any services are unhealthy. Contact the Cisco Technical Assistance Center (TAC) to remediate any issues before continuing.

Perform the following procedure as a user with customer support privileges:

1. In the Cisco Tetration GUI, click the Settings button and choose Maintenance.
2. In the left pane, click Upgrade.



3. Click Send Patch Upgrade Link. The patch upgrade link will be sent in an email message to the user. After the link has been sent successfully, a notification message will pop up.

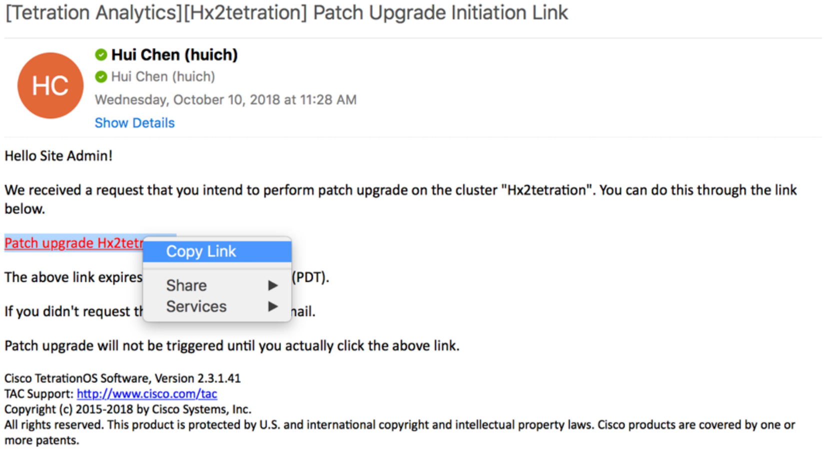


An email with the patch upgrade link has been sent successfully!

Operation: IDLE

Upgrade/Reboot can be initiated below

4. Check your inbox for the email message and follow the included instructions to upgrade the Cisco Tetration appliance. After you start a full upgrade, you may experience multiple hours of downtime.



[Tetration Analytics][Hx2tetration] Patch Upgrade Initiation Link

Hui Chen (huich)
Hui Chen (huich)
Wednesday, October 10, 2018 at 11:28 AM

Hello Site Admin!

We received a request that you intend to perform patch upgrade on the cluster "Hx2tetration". You can do this through the link below.

Patch upgrade Hx2tetr

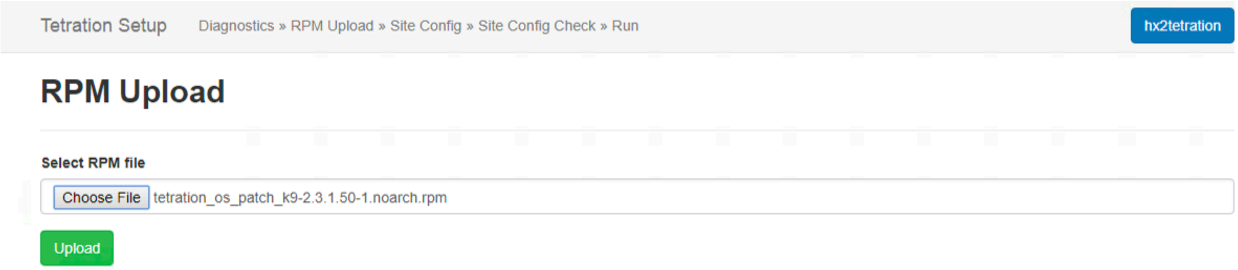
The above link expires (PDT).

If you didn't request th nail.

Patch upgrade will not be triggered until you actually click the above link.

Cisco TetrationOS Software, Version 2.3.1.41
TAC Support: http://www.cisco.com/tac
Copyright (c) 2015-2018 by Cisco Systems, Inc.
All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Cisco products are covered by one or more patents.

5. In the email message, click the upgrade link. The link opens the Cisco Tetration Setup GUI.
6. Click Choose File. Navigate to the patch RPM, choose it, and click Open.
7. Click Upload.

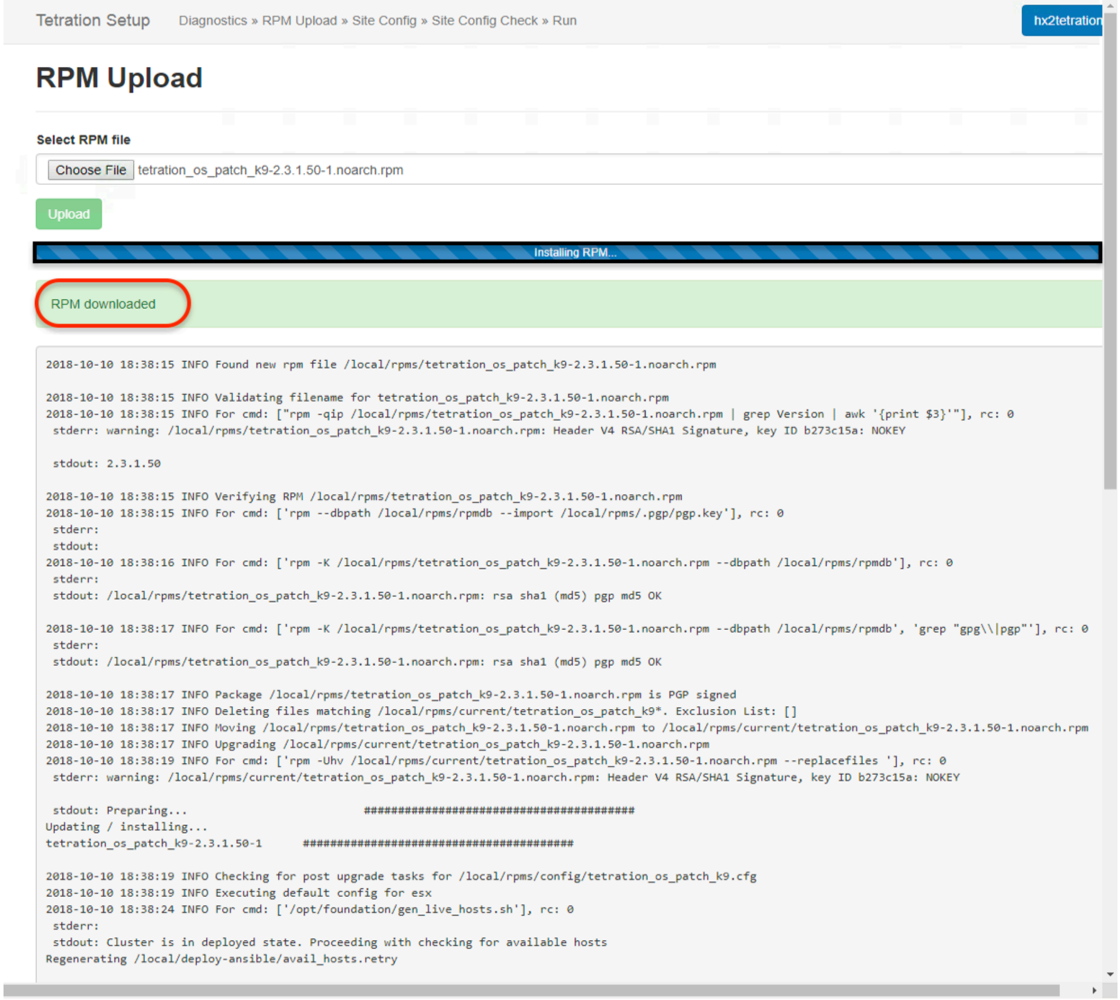


RPM Upload

Select RPM file: tetration_os_patch_k9-2.3.1.50-1.noarch.rpm

Tetration Setup
Diagnostics » RPM Upload » Site Config » Site Config Check » Run
hx2tetration
Choose File
Upload

8. The message " RPM downloaded" will appear if the upload is successful. The RPM installation process will then begin.


Tetration Setup
Diagnostics » RPM Upload » Site Config » Site Config Check » Run
hx2tetration

RPM Upload

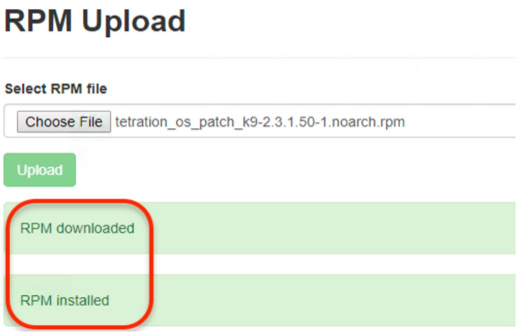
Select RPM file

tetration_os_patch_k9-2.3.1.50-1.noarch.rpm

RPM downloaded

```
2018-10-10 18:38:15 INFO Found new rpm file /local/rpms/tetration_os_patch_k9-2.3.1.50-1.noarch.rpm

2018-10-10 18:38:15 INFO Validating filename for tetration_os_patch_k9-2.3.1.50-1.noarch.rpm
2018-10-10 18:38:15 INFO For cmd: ["rpm -qip /local/rpms/tetration_os_patch_k9-2.3.1.50-1.noarch.rpm | grep Version | awk '{print $3}'"], rc: 0
 stderr: warning: /local/rpms/tetration_os_patch_k9-2.3.1.50-1.noarch.rpm: Header V4 RSA/SHA1 Signature, key ID b273c15a: NOKEY

 stdout: 2.3.1.50

2018-10-10 18:38:15 INFO Verifying RPM /local/rpms/tetration_os_patch_k9-2.3.1.50-1.noarch.rpm
2018-10-10 18:38:15 INFO For cmd: ['rpm --dbpath /local/rpms/rpmdb --import /local/rpms/.pgp/pgp.key'], rc: 0
 stderr:
 stdout:
2018-10-10 18:38:16 INFO For cmd: ['rpm -K /local/rpms/tetration_os_patch_k9-2.3.1.50-1.noarch.rpm --dbpath /local/rpms/rpmdb'], rc: 0
 stderr:
 stdout: /local/rpms/tetration_os_patch_k9-2.3.1.50-1.noarch.rpm: rsa sha1 (md5) pgp md5 OK

2018-10-10 18:38:17 INFO For cmd: ['rpm -K /local/rpms/tetration_os_patch_k9-2.3.1.50-1.noarch.rpm --dbpath /local/rpms/rpmdb', 'grep "gpg\\|pgp"'], rc: 0
 stderr:
 stdout: /local/rpms/tetration_os_patch_k9-2.3.1.50-1.noarch.rpm: rsa sha1 (md5) pgp md5 OK

2018-10-10 18:38:17 INFO Package /local/rpms/tetration_os_patch_k9-2.3.1.50-1.noarch.rpm is PGP signed
2018-10-10 18:38:17 INFO Deleting files matching /local/rpms/current/tetration_os_patch_k9*. Exclusion List: []
2018-10-10 18:38:17 INFO Moving /local/rpms/tetration_os_patch_k9-2.3.1.50-1.noarch.rpm to /local/rpms/current/tetration_os_patch_k9-2.3.1.50-1.noarch.rpm
2018-10-10 18:38:17 INFO Upgrading /local/rpms/current/tetration_os_patch_k9-2.3.1.50-1.noarch.rpm
2018-10-10 18:38:19 INFO For cmd: ['rpm -Uhv /local/rpms/current/tetration_os_patch_k9-2.3.1.50-1.noarch.rpm --replacefiles '], rc: 0
 stderr: warning: /local/rpms/current/tetration_os_patch_k9-2.3.1.50-1.noarch.rpm: Header V4 RSA/SHA1 Signature, key ID b273c15a: NOKEY

 stdout: Preparing...                          ########################################
Updating / installing...
tetration_os_patch_k9-2.3.1.50-1      ########################################

2018-10-10 18:38:19 INFO Checking for post upgrade tasks for /local/rpms/config/tetration_os_patch_k9.cfg
2018-10-10 18:38:19 INFO Executing default config for esx
2018-10-10 18:38:24 INFO For cmd: ['/opt/foundation/gen_live_hosts.sh'], rc: 0
 stderr:
 stdout: Cluster is in deployed state. Proceeding with checking for available hosts
Regenerating /local/deploy-ansible/avail_hosts.retry
```

9. Wait for the installation to be complete. The message " RPM installed" will appear. The whole process will take about 30 to 40 minutes.



RPM Upload

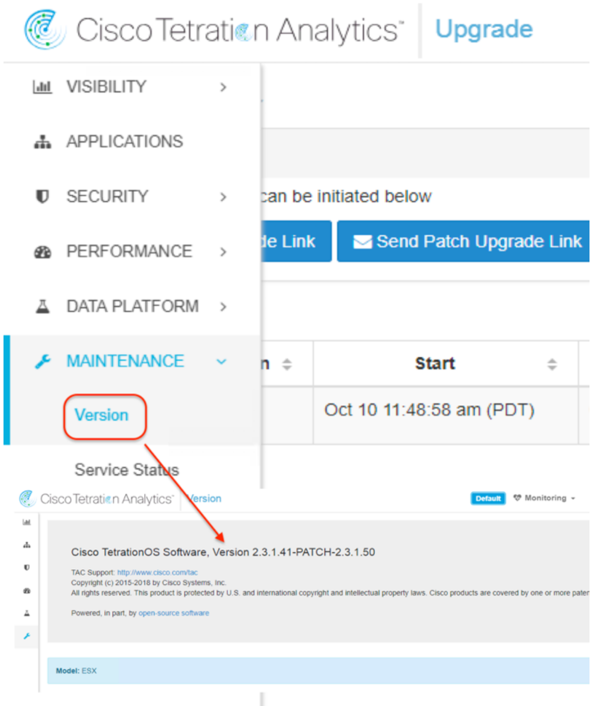
Select RPM file

tetration_os_patch_k9-2.3.1.50-1.noarch.rpm

RPM downloaded

RPM installed

10. Verify the upgrade.
    - In the Cisco Tetration GUI, click the Settings button and choose Maintenance. In the navigation pane, click Version. The newly installed TetrtationOS Software version will be displayed.



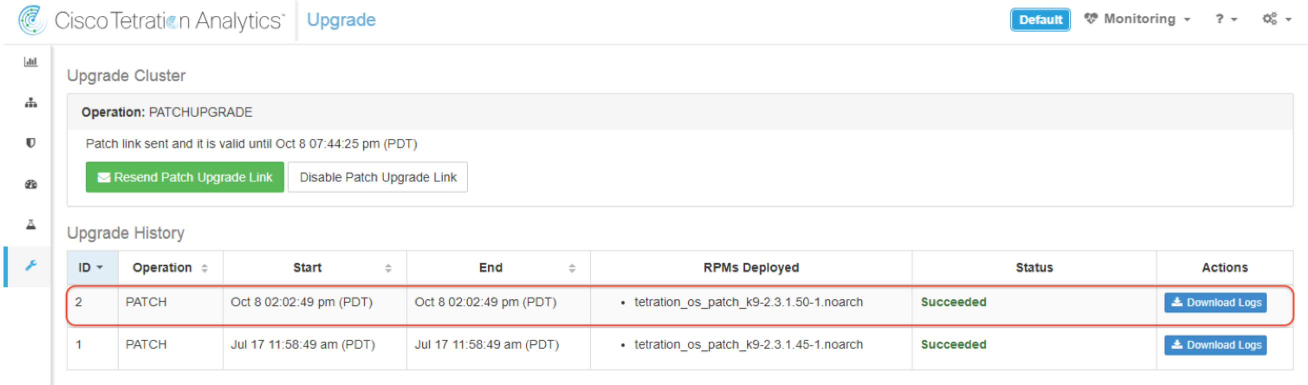
Cisco TetrationOS Software, Version 2.3.1.41-PATCH-2.3.1.50

TAC Support: http://www.cisco.com/tac
Copyright (c) 2015-2018 by Cisco Systems, Inc.
All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Cisco products are covered by one or more pater

Powered, in part, by open-source software

Model: ESX

- Alternatively, in the navigation pane, go back to the Upgrade page. In the Upgrade History section, you should see an upgrade status of Succeeded.


Cisco Tetration Analytics
Upgrade
Default
Monitoring
?
Resend Patch Upgrade Link
Disable Patch Upgrade Link

Upgrade Cluster

Operation: PATCHUPGRADE

Patch link sent and it is valid until Oct 8 07:44:25 pm (PDT)

Upgrade History

ID	Operation	Start	End	RPMs Deployed	Status	Actions
2	PATCH	Oct 8 02:02:49 pm (PDT)	Oct 8 02:02:49 pm (PDT)	• tetration_os_patch_k9-2.3.1.50-1.noarch	Succeeded	Download Logs
1	PATCH	Jul 17 11:58:49 am (PDT)	Jul 17 11:58:49 am (PDT)	• tetration_os_patch_k9-2.3.1.45-1.noarch	Succeeded	Download Logs

11. Click Disable Patch Upgrade Link and choose Yes to confirm. Then close the Tetration Setup GUI window before initiating another upgrade.

Conclusion

The Cisco Tetration-V virtual appliance provides an option that gives customers the benefits of the Cisco Tetration platform in a cloud-based or VMware ESXi-based virtualized environment. Cisco HyperFlex systems provide optimized hyperconverged infrastructure for any workload at any scale. This infrastructure provides an excellent choice of hardware and storage for the high-performing virtual infrastructure required for a Tetration-V deployment. Cisco HyperFlex systems simplify the Tetration-V deployment process and establish a solid foundation for data center analytics solutions.

For more information

For additional information, see the following:

- Cisco HyperFlex products, services, and solutions: https://www.cisco.com/go/hyperflex
- Cisco Tetration products, services, and solutions: https://www.cisco.com/go/tetration
- The latest Cisco Tetration Analytics virtual appliance deployment guide
- The latest Cisco Tetration Analytics upgrade guide

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA

C11-741621-00 12/18