Overview

Overview of Cisco Intersight Virtual Appliance

About Cisco Intersight Virtual Appliance

Cisco Intersight Virtual Appliance delivers the management features of Intersight in an easy to deploy VMware OVA, Microsoft Hyper-V Server VM, and KVM hypervisor. Intersight Virtual Appliance provides the benefits of Cisco Intersight that offers an intelligent level of management to enable customers to analyze, simplify, and automate their environments in more advanced ways than the previous generations of tools, while allowing more flexibility with additional data locality, security, and compliance requirements.

You can deploy Intersight Virtual Appliance in one of the following modes:

- Intersight Connected Virtual Appliance
- Intersight Private Virtual Appliance

Intersight Connected Virtual Appliance delivers the management features of Intersight while allowing you to control what system details leave your premises. Intersight Connected Virtual Appliance deployments requires a connection back to Cisco and Intersight services for automatic updates and access to services for full functionality.

Intersight Private Virtual Appliance delivers the management features of Intersight and allows you to ensure that no system details leave your premises. Intersight Private Virtual Appliance deployments is intended for an environment where you operate data centers in a disconnected (air gapped) mode.

For an overview of Intersight Assist, see About Cisco Intersight Assist, on page 13.

You can deploy Intersight Virtual Appliance as a single-node virtual machine in your existing environment.

You can also deploy Intersight Virtual Appliance on VMware vSphere as a multi-node cluster which allows for high availability. Once you have completed the initial set up of the single-node appliance, you can add additional nodes. After you successfully add two additional nodes, you can create a multi-node cluster in Intersight Virtual Appliance.

This guide provides an overview of how to install and set up Intersight Virtual Appliance in your environment.

Attention Before installing and setting up Intersight Virtual Appliance, it is strongly recommended that you read the information provided in the VM Resource Requirements for New Intersight Virtual Appliance Deployments section.

For latest updates on Intersight features and functionality, see Intersight Appliance Help Center.

Licensing Requirements for Intersight Virtual Appliance

Cisco Intersight Virtual Appliance uses a subscription-based license that is required to use the features of the appliance. Intersight Essentials is a subscription license delivered via **Cisco Smart Licensing**. Please contact your Cisco sales representative, channel partner, or reseller to purchase Intersight Essentials. Enabled platforms are those Cisco UCS and Cisco HyperFlex systems with a Cisco Intersight device connector, including eligible Cisco UCS Manager, Cisco IMC, and Cisco HyperFlex software.

For a **Connected Virtual Appliance** deployment, you must register the license as part of the initial setup of Cisco Intersight Virtual Appliance. After you complete the installation of the appliance, launch the UI and log in with the password that you set during installation, connect the appliance to Intersight, and register the license.

Use the following instructions if you want to edit the settings after the initial setup:

1. In the appliance UI, from the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **Licensing** > **Register License**.

   The **Smart Software Licensing Product Registration** window displays.

2. Generate a Product Instance Registration Token from your specific virtual account in **Cisco Smart Software Manager**, if you do not have one already.

3. Enter the Product Instance Registration Token that you obtained from **Cisco Smart Software Manager** and click **Register**. Click here to watch a video about Cisco Intersight licensing tiers and registration.

For a **Private Virtual Appliance** deployment, you must reserve the license as part of the initial setup of Cisco Intersight Virtual Appliance. For information on how to reserve a license as part of the initial setup, see Setting Up Single-Node Intersight Private Virtual Appliance.

For instructions on how to **update** or **return** the license after the initial setup of your Private Virtual Appliance, see Updating Intersight Private Virtual Appliance License and Returning Intersight Private Virtual Appliance License.

You can obtain an Intersight evaluation license for Cisco Intersight Virtual Appliance from your Cisco sales representative, channel partner, or reseller. If you already have a Cisco Smart Account, the evaluation license will be added to your Cisco Smart Account. You can then generate a token for the virtual account in the Smart account and proceed with registering Cisco Intersight Virtual Appliance. For more information about how to activate and manage your license, and learn more about Smart Licenses, see Managing Smart Licenses.

For a complete understanding of **Reserve Licenses** feature in Cisco Smart Software Manager, see Introduction to Smart Software Manager.

System Requirements

Supported Configuration Limits for Intersight Virtual Appliance

Cisco Intersight Virtual Appliance is available in multiple deployment sizes to support the scaling requirements of your environment. You can deploy the Appliance as follows:

New Deployments—You can deploy Intersight Virtual Appliance in medium or large configuration. Before selecting the size, assess your resource requirements and choose an appropriate option in the Intersight Appliance Maintenance Shell, and select the required size to deploy. The selected size will be deployed when the appliance VM restarts. For information about resource requirements, see VM Resource Requirements for New Intersight Virtual Appliance Deployments.

The following table lists the supported configuration limits:

Items	Configuration Limits		
	Small (Supported on existing deployments only)	Medium	Large
Number of Servers	2000	5000	8000
Number of Intersight Managed Mode (IMM) Domains (FI)	4	Up to 32	64
Number of Intersight Managed Mode (IMM) Servers	170 (metrics collection is not supported on small deployments)	500 (with metrics collection enabled)	2000 (with metrics collection enabled)
		5000 (with metrics collection disabled)	8000 (with metrics collection disabled)
Number of UCSM Managed Mode (UMM) Domains	30	500	800
Number of UCSM Managed Mode (UMM) Servers	330	Up to 5000	8000
Number of UCS Standalone Rack Servers	1500	5000	8000
Number of parallel HyperFlex Installations	2	5	5
Number of Supported Concurrent Operations	50	100	100
Number of Concurrent User Sessions (GUI and API)	32	32	32

VM Resource Requirements for New Intersight Virtual Appliance Deployments

The Cisco Intersight Virtual Appliance can be deployed on VMware ESXi 7.0 or later, Microsoft Hyper-V Server 2016 and 2019, and KVM hypervisor on Linux. You can deploy Intersight Virtual Appliance in Medium or Large configuration.

For more information on the supported maximum configuration limits for Intersight Virtual Appliance Sizing Options, see Supported Configuration Limits for Intersight Virtual Appliance.

Table 1: Resource Requirements for New Intersight Virtual Appliance Deployments

Resource	Requirements	
	Medium	**Large**
vCPU (AVX Required)	24	48
RAM	64 GiB	96 GiB
Storage (Disk)	2 TiB*	2 TiB*
Supported Hypervisors	VMware ESXi 7.0 or later with VMware vSphere Web Client 7.0 or later Microsoft Hyper-V Server 2016 and 2019 KVM hypervisor on Linux	

*Cisco recommends that you use thick provisioning. While it is possible to use thin provisioning, over-provisioning can lead to a lack of storage capacity which can then result in degradation and loss of service, and might require a restore from backup.

Small configuration is still supported on existing deployments. For more information, see VM Resource Requirements for Existing Intersight Virtual Appliance Deployments, on page 5.

Attention

- Do not change the default settings for disk sizes while installing Intersight Virtual Appliance on VMware vSphere. The disk sizes are computed based on the deployment configuration.
- It is mandatory to have a CPU that supports the AVX feature. If you have the Enhanced vMotion Compatibility (EVC) level configured for your VMware vSphere cluster, ensure that the EVC level is set to a CPU family that supports the AVX feature.
- If the allocated resources fall below the default values required for a Medium deployment (24 for vCPU and 64 GiB for RAM), then Assist will be the only option available for deployment. Other options will be grayed out.
- **Metric collection:**
  - Metric collection is an opt-in feature and is currently supported on single-node deployments only. For information on how to configure metrics collection, see Configuring Metrics Collection.
  - When metrics collection is enabled, you can claim a maximum of 500 IMM servers for medium configuration and a maximum of 2000 IMM servers for large configuration. However, you can claim additional UMM servers up to the supported limits for medium and large configuration.
  - When the active server count for which metrics is collected, exceeds the threshold that your appliance size can support, be it medium or large, Intersight Virtual Appliance automatically disables metrics collection. This precaution is taken to prevent any negative impacts on performance, allowing for smooth system operation without the need for manual intervention. Once the metrics collection is disabled, you will have to enable it manually, after the resource requirements are met for this feature.
  - Any metrics that have been collected while the metrics collection was enabled will remain accessible, even if metrics collection is later paused. This ensures the continued availability of a historical data set for future analysis and reference. Enforcement of the storage and retention policies for metrics continues, even when the metrics collection is disabled.
  - For more information about metrics collection, see Monitoring Overview.
- **Additional Networking Requirements for Multi-node Deployments:**
  - Disk write speed must be greater than 150 megabytes per second.
  - Latency between nodes must be less than 9 milliseconds.
  - All three hostnames for the nodes must be resolved by the same set of DNS servers.

VM Resource Requirements for Existing Intersight Virtual Appliance Deployments

Intersight evaluates the changes that are required in the CPU, RAM, and disk to determine the deployment size during the reboot after an update from the cloud service. As a result of the evaluation, one of the following outcomes occurs:

- If the minimum required resources for a particular deployment size are not available, the Intersight services are shut down and the appliance remains powered on. However, the appliance may not be functional and the services running could be unstable. Intersight Appliance Maintenance Shell displays an error message regarding the resource status during the reboot. Log in to the Maintenance Shell to learn more about the error and the required remedial actions.

- If the deployment size is same as the existing deployment, the VM restarts without any change. You can upgrade to a higher deployment size after determining resource requirements.

Table 2: Resource Requirements for Existing Intersight Virtual Appliance Deployments

Resource	Requirements		
	Small	**Medium**	**Large**
vCPU (AVX Required)	16	24	48
RAM	32 GiB	64 GiB	96 GiB
Storage (Disk)	Minimum of 620 GiB* (applicable starting with Appliance Release Version 1.0.9-631)	2 TiB*	2 TiB*
Supported Hypervisors	VMware ESXi 7.0 or later with VMware vSphere Web Client 7.0 or later Microsoft Hyper-V Server 2016 and 2019 KVM hypervisor on Linux		

Note

- *Cisco recommends that you use thick provisioning. While it is possible to use thin provisioning, over-provisioning can lead to a lack of storage capacity which can then result in degradation and loss of service, and might require a restore from backup.
- It is mandatory to have a CPU that supports the AVX feature. If you have the Enhanced vMotion Compatibility (EVC) level configured for your VMware vSphere cluster, ensure that the EVC level is set to a CPU family that supports the AVX feature.
- Complex sort and filter functionality is available only on medium and large deployments. Small deployments support the sort and filter functionality on just a few columns.

Managing Resources for Intersight Virtual Appliance Deployments

Managing Resources for Intersight Virtual Appliance Deployments

You can view the deployment size of Intersight Virtual Appliance and make changes to CPU, RAM, and disk size as follows:

1. From the **Service Selector** drop-down list, choose **System**.
2. Navigate to **Settings** > **GENERAL > Appliance** .
3. Review the other supported scaling options and choose the appropriate deployment size to suit your requirement.
4. After you review the details of the resource requirement for a supported deployment option, shut down the VM, change the CPU, RAM, and disk size as required, and restart the VM.

Note

- You cannot change the disk sizes when you have a snapshot.
- To use the Virtual Appliance sizing options, you must have the latest upgrades from the Intersight cloud service.

The following table provides information about the disk size requirements for Intersight Virtual Appliance installations.

Table 3: Disk Size Requirements for Intersight Virtual Appliance Installations

Disk	Minimum Disk Size Requirements for all Deployments	Recommended Disk Size Requirements for Medium and Large Deployments
Disk1	Do not change the disk size.	Do not change the disk size.
Disk2	25 GiB	25 GiB
Disk3	150 GiB	150 GiB
Disk4	150 GiB	150 GiB
Disk5	100 GiB	190 GiB
Disk6	30 GiB	60 GiB
Disk7	60 GiB	360 GiB
Disk8	60 GiB	1190 GiB

Note Alternatively, you can meet the disk requirements by performing a restore using the latest backup of the appliance. For more information, see Recovering Intersight Connected Virtual Appliance and Recovering Intersight Connected Virtual Appliance.

IP Address and Hostname Requirements

IP Address and Hostname Requirements for Intersight Virtual Appliance

Setting up a single-node Intersight Virtual Appliance requires an IP address and 2 DNS records for that IP address. The DNS records must be in the following formats:

- **myhost.mydomain.com**—A DNS record in this format is used to access the GUI. This must be defined as an **A record and associated PTR record** in DNS. The PTR record is required for reverse lookup of the IP address. If an IP address resolves to multiple hostnames, the first resolved hostname is used.
- **dc-myhost.mydomain.com**—The **dc-** must be prepended to your hostname. This DNS record must be defined as the **CNAME of myhost.mydomain.com**. DNS records in this format are used internally by the appliance to manage target connections.

Setting up a multi-node cluster for Intersight Virtual Appliance requires three hostnames, three IP addresses, and one DC-CNAME for each hostname. The following is an example of the formats:

- **myhost1.mydomain.com**
- **myhost2.mydomain.com**
- **myhost3.mydomain.com**
- **dc-myhost1.mydomain.com**
- **dc-myhost2.mydomain.com**
- **dc-myhost3.mydomain.com**

Attention Ensure that the appropriate entries of type **A, CNAME, and PTR records** exist in the DNS, as described above.

Reserved IP Address Range Requirements

Intersight Virtual Appliance reserves the following IP address ranges for internal communication:

- **/20 subnet within the 172.16.0.0/12 range**—This subnet is one-time configurable during the appliance installation.
- **192.168.20.21/32**—This IP address is reserved by the appliance and is non-configurable.

Port Requirements

Port Requirements for Intersight Virtual Appliance

The following table lists the ports that are required for Intersight Virtual Appliance communication.

Port	Protocol	Appliance Configuration Mode	Description
443	TCP	Single-node and multi-node	This port is required for communication between: • **Intersight Virtual Appliance and the users' web browser.** • **Intersight Virtual Appliance to and from the endpoint targets.** For more information about connectivity, see the Network Connectivity Requirements for Intersight Connected Virtual Appliance section.
53, 67, 68	UDP	Single-node and multi-node	These ports are used to send and receive DNS and NTP traffic.

Port	Protocol	Appliance Configuration Mode	Description
2379, 6443, 2380, 9092, 9094, 9100, 10250	TCP	Multi-node	These ports are used for communication between the VMs in a multi-node configuration for Intersight Virtual Appliance.
51820, 51821	UDP	Multi-node	These ports are used for securing VPN between the VMs in a multi-node configuration for Intersight Virtual Appliance.

Network Connectivity Requirements for Intersight Connected Virtual Appliance

Note The information in this section is applicable only for Intersight Connected Virtual Appliance deployments.

- Ensure that Cisco Intersight Virtual Appliance has access to the following sites directly or through a proxy. For more information about setting up a proxy, see Cloud Connection for Intersight Connected Virtual Appliance. All the following URLs are accessed through HTTPS.
  - Access to Cisco services (*.cisco.com).

Cisco Service	Description	Target Device
smartreceiver.cisco.com:443	For access to Cisco Smart Licensing Manager	Required for all servers
swapi.cisco.com:443	For access to Cisco Smart Licensing Manager	Required for all servers
tools.cisco.com:443	For access to Cisco Smart Licensing Manager	Required for all servers
download-ssc.cisco.com*, dl.cisco.com, dl1.cisco.com, dl2.cisco.com	For access to Cisco Software download site	Required for the following: • C-Series Standalone Servers • UCSM Managed B-Series and C-Series servers • UCSM Managed Fabric Interconnects • UCSM Managed Fabric Interconnects-attached Cisco UCS S3260 Chassis
api.cisco.com:443		
cloudsso.cisco.com:443		

* Cisco Intersight allows you to manage firmware downloads through a new domain *download-ssc.cisco.com*. Make sure that you add this new domain to the firewall and network rules. For more information, see Cisco Software Download.

- Access to Intersight Cloud services.

  Intersight Virtual Appliance connects to Intersight by resolving one of the following URLs:

Note IP address for any given URL could change. In case you need to specify firewall configurations for URLs with fixed IPs. The following are the static IP addresses corresponding to each region.

North America (us-east-1) region

- svc-static1.intersight.com **(Preferred)**.
- svc-static1.ucs-connect.com **(Will be deprecated in the future)**.
- Both these URLs resolve to the following IP addresses:
  - 3.208.204.228
  - 54.165.240.89
  - 3.92.151.78

EMEA (eu-central–1) region

- svc.eu-central-1-static1.Intersight.com
- This URL resolves to the following IP addresses:
  - 99.84.238.166
  - 99.84.238.204
  - 99.84.238.94
  - 99.84.238.110

Requirements for Successful Target Connection to Intersight Virtual Appliance

For a successful target connection to Intersight Virtual Appliance, ensure that the following connectivity requirements are met:

- Ensure that a network connection can be established from the Device Connector to the appliance.
- The Device Connector establishes an HTTPS connection to <*https://dc-fqdn-of-your-appliance*> and then upgrades the HTTPS connection to a web socket. Ensure that your security rules allow the device connector to establish a web socket connection.
- Ensure that **Intersight Management** is enabled in the device connector (it is enabled by default). You can find **Intersight Management** in **Admin** > **Device Connector** > **Intersight Management** in Cisco

UCS Manager/Cisco UCS Director/Cisco IMC, and **Settings** > **Device Connector** in the Cisco HyperFlex UI.

- Check if a firewall is introduced between the managed target and the appliance, or if the rules for an existing firewall have changed, thus affecting connectivity. If the rules are changed, ensure that the changed rules permit traffic through the firewall.
- Ensure that all applicable physical and Virtual IPs are allowed through the firewall.
- If you use an HTTP proxy to route traffic out of your premises, and if you have made changes to the HTTP proxy server's configuration, ensure that you change the device connector's configuration accordingly. This is required because the appliance does not automatically detect HTTP proxy servers.
- Configure DNS and resolve the DNS name. The Device Connector must be able to send DNS requests to a DNS server and resolve DNS records. The Device Connector must be able to resolve *dc-<fqdn-of-your-appliance>* to an IP address.
- Configure NTP and validate that the target time is properly synchronized with a time server.

Note When the target time is not properly synchronized, the Device Connector may be unable to establish a secure connection to the appliance and the TLS certificate may be considered invalid.

Attention You must configure DNS and NTP on the management interface (Cisco UCS Manager/Cisco IMC/Cisco HyperFlex) and not on the Device Connector UI.

- You must configure security targets that are in the network path by enabling network connectivity to the appliance.
- The Intersight Device Connector uses Amazon Trust Services to validate certificates. If you wish to leverage certificate validation, you must open port 80 and allow communication to amazontrust.com in your firewall settings. Allowing for certificate validation is optional but recommended.

Important Intersight uses the Online Certificate Status Protocol (OCSP) and Certificate Revocation Lists (CRL) servers to validate HTTPs certificates. These protocols are designed to distribute the revocation status over HTTP. CRLs and OCSP messages are public documents that indicate the revocation status of X.509 certificates. They are generated by the Certificate Authority that issues the certificates. To prevent spoofing, CRLs and OCSP messages are digitally signed by the Certificate Authority. Since the revocation status data is public and signed, there is no need to protect the CRL/OCSP connection with HTTPs.

A PKI client can query a CRL or use OCSP to verify a certificate prior to use. In particular, when a client establishes a TLS session to a server, it can determine the certificate revocation status of the X.509 certificate presented by the server. If the certificate is valid the TLS connection can proceed. If the certificate has been revoked, the client must terminate the TLS connection. The original TLS connection triggers a CRL or OCSP lookup, which in turns triggers another connection to get the revocation status. If that secondary connection were to be done over HTTPs, that itself could trigger another connection to check the revocation status recursively.

Supported Browsers

Supported Browsers for Intersight Virtual Appliance

Cisco Intersight runs on the following minimum supported browser versions:

- Google Chrome 62.0.3202.94
- Firefox 57.0.1
- Safari 10.1.1
- Microsoft Edge (Chromium) Beta

Software Compatibility

Software Compatibility for Intersight Virtual Appliance

This section contains details about the minimum versions of the following software supported by the appliance:

Component	Minimum Supported Version
Cisco UCS Manager	3.2(1)
Cisco HyperFlex Connect and Data Platform	2.6

Component	Minimum Supported Version
Cisco IMC	3.1(3) for M5 Servers 3.0(4) for M4 Servers For more information about the Cisco IMC Software requirements for the M4 and M5 Servers, see the Supported Systems section in the Help Center. See Device Connector Requirements. for a complete list of the supported software and the required device connector versions.
Cisco UCS Director	6.7.2.0
Cisco Intersight Managed Mode	4.1(2a)

Overview of Cisco Intersight Assist

About Cisco Intersight Assist

Cisco Intersight Assist helps you add endpoint devices to Cisco Intersight. A datacenter could have multiple devices that do not connect directly with Cisco Intersight. Any device that is supported by Cisco Intersight but does not connect directly with it, will need a connection mechanism. Cisco Intersight Assist provides that connection mechanism, and helps you add devices into Cisco Intersight.

Cisco Intersight Assist enables Cisco Intersight to communicate with targets that do not have a direct path to Cisco Intersight and do not have an embedded Intersight Device Connector. These include targets such as Storage Devices, Hypervisor Managers, Application Performance Management products, and much more. Intersight Assist communicates with the target's native APIs and serves as the communication bridge to and from Cisco Intersight. Intersight Assist services run as a standalone appliance when used with Cisco Intersight SaaS. For Connected Virtual Appliance and Private Virtual Appliance, a separate Assist Appliance is not needed as the services are collocated.

You can view the Intersight Assist details by navigating to **Appliance UI** > **Target**.

You can choose to install Cisco Intersight Assist from the installer during the set-up wizard. It can be installed on an ESXi server, Kernel-based Virtual Machine (KVM), and HyperV Hypervisors.

Note You cannot de-register Intersight Assist, and you cannot claim another Intersight Assist with the appliance.

After claiming Intersight Assist into Cisco Intersight, you can claim endpoint devices using the **Claim Targets** option. For more information, see Claim Targets.

Note Cisco Intersight Assist does not support IPv6 configurations.

Now, you can add Pure Storage devices, Hitachi Virtual Storage Platform devices, NetApp storage controllers, VMware vCenter, and much more devices into Cisco Intersight after claiming them using Cisco Intersight Assist.

Licensing Requirements for Intersight Assist

For more information on licensing, see Intersight Licensing.

System Requirements For Intersight Assist

VM Resource Requirements for Intersight Assist

You can deploy Cisco Intersight Assist on Kernel-based Virtual Machine (KVM), HyperV Hypervisors, and VMware ESXi 7.0 or later with VMware vSphere Web Client 7.0 or later Microsoft Hyper-V Server 2016 and 2019. This section describes the system requirements to install and deploy Cisco Intersight Assist. You can deploy Intersight Assist in Small, Medium, and Large options.

New Deployments—You can deploy Intersight Virtual Appliance in Small, Medium, or Large configuration.

Existing Deployments—Existing deployments are supported for Tiny, Small, Medium, and Large configuration. However, it is **recommended** that you migrate existing Tiny deployments to Small, Medium, or Large configuration.

Note
- Tiny deployment is supported only for existing Assist deployments and is applicable only for Intersight Orchestrator.

Table 4: Intersight Assist Resource Requirements

Resource	Requirements			
	Tiny (Supported for existing deployments only)	**Small**	**Medium**	**Large**
vCPU (AVX Required)	8	16	24	48
RAM	16 GiB	32 GiB	64 GiB	96 GiB
Supported Features	ICO and IKS	ICO, IWO, IST, and IKS	ICO, IWO, IST, and IKS	ICO, IWO, IST, and IKS

Resource	Requirements
Supported Hypervisors	VMware ESXi 7.0 and higher VMware vSphere Web Client 7.0 and higher Kernel-based Virtual Machine (KVM) HyperV Hypervisors

Note

- It is mandatory to have a CPU that supports the AVX feature. If you have the Enhanced vMotion Compatibility (EVC) level configured for your VMware vSphere cluster, ensure that the EVC level is set to a CPU family that supports the AVX feature.

This following table lists the system requirements to deploy Cisco Intersight Assist for Intersight Workload Optimizer.

Table 5: Intersight Assist Resource Requirements for Intersight Workload Optimizer

Resource Requirement	System Requirements		
	Small	**Medium**	**Large**
vCPU (AVX Required)	16	24	48
RAM	32 GiB	64 GiB	96 GiB
Storage (Disks)	500 GiB	500 GiB/2TiB*	2 TiB*
Deploy Configuration	Up to 1000 Virtual Machines	Up to 30,000 Virtual Machines	Up to 100,000 Virtual Machines

Note

- *Existing deployments can upgrade from **Small** configuration to **Medium** configuration by either remaining at 500 GiB or upgrading to 2 TiB.
- *New deployments for **Medium** and **Large** configuration will be supported only with full 2 TiB disk size configuration.
- It is mandatory to have a CPU that supports the AVX feature. If you have the Enhanced vMotion Compatibility (EVC) level configured for your VMware vSphere cluster, ensure that the EVC level is set to a CPU family that supports the AVX feature.

This following table lists the resource requirements to deploy Cisco Intersight Assist for Intersight Service for HashiCorp Terraform Service (IST).

Table 6: Intersight Assist Resource Requirements for Intersight Service for HashiCorp Terraform Service (IST)

Resource	Requirements		
	Small	**Medium**	**Large**
vCPU (AVX Required)	16	24	48
RAM	32 GiB	64 GiB	96 GiB
Number of Terraform Agents	5	5	5

Note

- It is mandatory to have a CPU that supports the AVX feature. If you have the Enhanced vMotion Compatibility (EVC) level configured for your VMware vSphere cluster, ensure that the EVC level is set to a CPU family that supports the AVX feature.

Port Requirements for Intersight Assist

The following table lists the port numbers that must be open for Cisco Intersight Assist communication.

Port	Protocol	Description
443	TCP/UDP	Required for communication between: • Cisco Intersight Assist and the user's web browser. • Cisco Intersight Assist to and from the endpoint devices.

Supported Browsers for Intersight Assist

Cisco Intersight Assist and Cisco Intersight runs on the following minimum supported browser versions:

- Google Chrome 62.0.3202.94
- Firefox 57.0.1
- Safari 10.1.1
- Microsoft Edge (Chromium) Beta