Cisco Secure Workload Virtual (Tetration-V) Deployment Guide

First Published: 2021-08-17

Last Modified: 2023-01-05

Deploying Secure Workload Virtual

About Deploying Secure Workload Virtual

Secure Workload Virtual (also known as Tetration-V) is a software solution for deploying Cisco Secure Workload (formerly known as Cisco Tetration) in the VMware ESXi environment.

For more information about Cisco Secure Workload, see https://www.cisco.com/c/en/us/products/security/tetration/index.html.

Limitations

- Beginning September 1, 2021:

  Secure Workload Virtual (Tetration-V) can be used only for proof of concept (POC) or proof of value (POV) in non-production environments.

  For purchases before September 1, 2021:

  Tetration-V was intended for small scale deployments or environments where virtualization is the only available compute option.

- Snapshots of VMs are not supported
- Hardware sensors are not supported with Secure Workload Virtual.

Prerequisites

To deploy the Secure Workload virtual appliance in the VMware ESXi environment, your set-up must meet the following requirements:

Software Prerequisites

- Hypervisor
  - VMware high availability cluster running a supported VMware vSphere version:
    - For Secure Workload version 3.6.x: VMware vSphere 6.5, 6.7, or 7.0.3
    - For Tetration versions through 3.5.x: VMware vSphere version 6.5 or 6.7

- vSphere 6.7U3 or later with HTML5 client for deployment is recommended
- The version requirement applies to all components, such as the hypervisors, core management, authentication and services, and upgrade and patch management
- The deployment must be running in a configuration supported by VMware
- All hosts must be part of a single HA cluster with Distributed Resource Scheduler (DRS) enabled

- The **Tetration virtual appliance install OVA for VMware ESXi environment** OVA file, available from the Software Downloads page on Cisco.com.
- Required Secure Workload (Tetration) RPMs, also available from the Software Downloads page on Cisco.com:
  - OS Adhoc
  - OS Enforcement

    (not applicable for releases earlier than 3.5.1.x)
  - OS Mother
  - OS OVA
  - OS RPMInstall

Hardware Prerequisites

- To ensure the highest performance, it is recommended to use dedicated hardware for the cluster.
- Infrastructure capable of hosting:
  - 128 physical CPU cores with a minimum of 2 GHz clock speed
  - 2 TB RAM
    - The virtual machines will be as large as 128 GB.
    - The memory cannot be overcommitted.
  - 18.1 TB Storage
    - The storage must be high performance, such as flash memory or SSD, that is capable of a minimum of 5,000 I/O operations per second (IOPS).
    - The storage must be accessible from all of the nodes in the cluster.
    - The storage must be provisioned as a single, shared VMware vSphere datastore. Hyperflex, vSAN, FC/FCoESAN, NFS, and iSCSI are supported.
    - The storage must be durable.
  - A resource check is performed at deployment, however the infrastructure must be managed to stay within requirements.
- Network infrastructure

- All hosts in the cluster should be connected with at least 10 Gigabit Ethernet (GbE) interfaces.
- All hosts must have three virtual networks available for Secure Workload purposes.
  - **Public Network** – Dedicated or shared public network for external cluster traffic that must be reachable from sensors and clients and have access to the vCenter. This network is used for Secure Workload application access. You must specify a minimum subnet of /28. If the external network is dedicated with the full range of IP addresses being available, then eight IP addresses are automatically consumed as shown in the following table:

    Table 1: IP Address in Range

IP Address	Description
1st	Gateway IP address (Reserved).
2nd and 3rd	Reserved
4th	Web UI virtual IP address.
5th	Sensor management virtual IP address.
6th	Collector.
7th	Collector.
8th	Application interface.
9th	Application interface.
10th	Adhoc-Kafka.
11th	Orchestrator; used as needed.

    If the public network is shared, you must define specific available addresses.
  - **Private Network** – Dedicated private network for internal cluster communication that must not be routable nor shared. You must specify a minimum subnet of /26. We recommend a subnet of /24.
  - **Configuration Network** – Temporary network for a bootstrapping cluster that must be reachable by the user who is performing the deployment, and must also have access to the VMware vCenter. This should be a separate subnet from the public subnet, and should be shut down after the deployment has completed. This network is used for Secure Workload setup interface access.
- VMware vSphere Distributed Switch (VDS)
  - The VDS may be native or Cisco ACI-controlled.
  - All hosts must have a consistent network configuration with a common VDS.
- If you use a VDS, it must include all of the hosts in the cluster.

Note Despite hardware recommendations being satisfied, no performance guarantee or SLA can be made since other factors may impact the overall performance of the Secure Workload software.

Network Connectivity / Firewall Requirements during deployment

During deployment, the bootstrap orchestrator will have two public facing IP addresses assigned:

- Configuration network
- Public network

Orchestrator will automatically assign the last address in the Public network, and use that for performing Site Checker validation. This includes (but is not limited to): SMTP, DNS, NTP, Ping, vCenter connection tests. After Site Checker validation has completed, orchestrator will remove the IP address, and continue the rest of deployment using the Configuration network. The following connectivity will be established:

Network	Destination	Protocol	Port
Config and Public	DNS server	UDP	53
Config and Public	NTP server	UDP	123
Public	SMTP server	TCP	SMTP Port
Config and Public	vCenter host	TCP	443
Config	ESXi Hosts* (see note below table)	TCP	443

* OVF tool establishes connectivity with vCenter, which redirects to ESX for large file transfers

After the deployment has completed, the Configuration network will remove its IP address and shut down the interface. Upgrades will be done entirely using the Public network.

SSH Public Key

You must have an SSH public key for remote support access to the Secure Workload platform if the GUI is unavailable. Before you begin installing the Secure Workload virtual appliance, generate an RSA 4096 bit key pair. You will specify this key during the installation. Keep the private key secure and available for future use.

Email Addresses

You must provide 3 unique email addresses that are used for initial system access and outbound alerting.

Table 2: Email Addresses

Email Address	Description
Site-Admin	This address is used to create a default administrator account.
Customer-Support	This address is used to create a default customer support account.

Email Address	Description
Alerts	This address is used for outbound alerts.

Recommended VMware Configuration Settings

Each VMware vSphere deployment can have different requirements, constraints, and best practices that the administrator has implemented. The Secure Workload installer does not make any configuration changes to the VMware vSphere deployment. The recommendations in this section should not replace the advice and careful planning of a VMware expert. If you do not follow these recommendations, the availability of the data might suffer and Secure Workload might not function completely or as intended.

The following list contains the recommended VMware configuration settings:

- Enable the VMware vSphere Distributed Resource Scheduler (DRS), VMware vSphere high availability (HA) for host failure, and VMware vMotion on the cluster where Secure Workload will be deployed. This will help provide availability and performance for instances in the Secure Workload cluster.
- Datastores must be highly available and durable, meaning that data is stored redundantly and is resistant to hardware failure.
- Set the hypervisor hosts and VMware vCenter server clocks correctly and synchronize the clocks using the Network Time Protocol (NTP).

After deployment, you will configure anti-affinity rules as described in the deployment procedure below.

VMware Permissions

The Secure Workload installer requires credentials to access VMware vSphere for creating virtual machines, folders, files in the Datastore, and to connect to virtual switches and datastores.

We strongly recommend that you use a separate user account for the Secure Workload installer, which has the minimum required permissions to perform the installation.

The following permissions can be used as a starting point for creating the VMware user account role:

- Content Library
- Datastore
- Folder\Create Folder
- Network\Assign network
- Resource
- Tasks
- Virtual Machine
- dvPort Group
- vApp
- vSphere Tagging (Labeling)

The open-source utility Terraform is used for managing some resources in vSphere. For more information on required permissions from Terraform, please see https://www.terraform.io/docs/providers/vsphere/index.html#notes-on-required-privileges.

Site Information

Your setup must meet the following site information requirements:

Network Tab

- **External Network**—The external network subnet, which must have at least 8 free IP addresses.
  - Unless you configure the external IP addresses in the **Advanced** tab, automatic assignment is used with the following rules:
    - Automatic assignment attempts to allocate the IP addresses automatically.
    - Automatic assignment skips the first 3 and last 3 IP addresses, and inclusively assigns the 4th IP address up through the 4th to last IP address.
    - The first usable IP address in the subnet is used as the gateway.

    For example, if you specify `192.168.1.0/28` for the subnet, `192.168.1.1` is the gateway and IP addresses `192.168.1.4` through `192.168.11` will be used.

ESX Tab

- **vSphere Host**—The IP address or hostname of the VMware vCenter server.
- **vSphere Username**—The username for the VMware vSphere account that has the necessary roles to upload files and create virtual machines.
- **vSphere Password**—The password for the VMware vSphere account.
- **vSphere Datacenter**—The name of target the VMware vSphere data center.
- **Cluster**—The cluster into which virtual machines will be placed.
- **VM Folder Name**—The name of the folder in which Secure Workload virtual machines will be placed. Nested folders are not supported.
- **Datastore**—The datastore into which virtual machines will be allocated for storage.
- **Private Network Port Group**—The name of the virtual switch port group to use for private networking.
- **Public Network**—The name of the virtual switch port group to use for public networking.
- **Cloud Init Folder**—The folder name on the datastore that will be used for storing the deployment configuration files.

Advanced Tab (Optional)

- **External IPs**—If a shared subnet will be used for the public network, specify the list of IP addresses that might be used by the deployment. The IP addresses must meet the following requirements:
  - 8 IP addresses are required.

- The first three IP addresses in a subnet cannot be specified.
- The first usable IP address in the subnet is used as the gateway.

For example, you can specify 8 IP addresses in the **192.168.1.0/24** subnet, but IP addresses **192.168.1.1** through **192.168.1.3** cannot be used. 192.168.1.1 is gateway.

External Service Parameters

The following table provides information about the external service parameters:

Table 3: External Service Parameters

Service	Parameters	Required/Optional
vCenter	vCenter Host User Credentials VM Folder Cluster and Data Center Names Port Groups—Orchestrator, Public, and Private Datastore Name	Required
DNS	One or more DNS servers	Required
NTP	One or more NTP servers	Required
SMTP	SMTP Host SMTP Port Authentication Credentials (optional)	Required
Proxy	HTTP Proxy Server and Port HTTPS Proxy Server and Port	Optional
Syslog	Syslog Server and Port	Optional

Cluster Parameters

The following table provides information about the cluster parameters:

Table 4: Cluster Parameters

Parameters	Required/Optional	Notes
Site Name	Required	You cannot change the name after deployment. The name must match the host portion of the UI FQDN.

Parameters	Required/Optional	Notes
UI FQDN	Required	The FQDN should be resolvable in the DNS.

Deploying the Secure Workload Virtual Appliance in the VMware ESXi Environment

The following procedure deploys the Secure Workload virtual appliance in the VMware ESXi environment. First, you deploy the orchestrator OVA, then you set up Secure Workload.

Procedure

Step 1 Log in to the VMware vSphere Web interface.

Step 2 Create a new Folder with the intended site name of the cluster.

Step 3 Right-click the target cluster and choose **Deploy OVF Template**.

Step 4 Enter the location of the OVF template.

We recommend that you host the orchestrator OVA on a Web server close to the ESX cluster. Because the orchestrator OVA is over 5GB, the file can take a long time to transfer on a slow link.

Step 5 Click **Next**.

Step 6 Enter **`orchestrator-1`** for the virtual machine name. Make sure that the virtual machine deploys in the intended data center and in the Secure Workload deployment folder named with the cluster site name.

Step 7 Click **Next**.

Step 8 Confirm that the chosen cluster is the intended target.

Step 9 Click **Next**.

Step 10 Review the licensing agreement, and if you agree to the terms, click **Accept**.

Step 11 Click **Next**.

Step 12 Use the default configuration profile (**2CPU-8GB**) and click **Next**.

Step 13 Choose the datastore that you want for the deployment. You can leave all other options at their default settings, unless the environment requires other settings.

Step 14 Click **Next**.

Step 15 Choose the appropriate network mapping.

- **Configuration**—Enter the routable network where the orchestrator can be reached during the deployment phase of the cluster bring up. Use a network that is different from the public network. Disconnect the network from **orchestrator-1** after the deployment has completed.
- **Private**—Enter the non-routed internal network that Secure Workload will use for internal communication.
- **Public**—Enter the routable network where the GUI, collectors, and virtual IP addresses will be reachable.

Step 16 Click **Next**.

Step 17 Enter the orchestrator reachability details for the configuration network.

- **IP address**—Enter the dotted quad notation of the IP address for the orchestrator.
- **Netmask**—Enter the dotted quad notation of the netmask for the network.
- **Gateway**—Enter the dotted quad notation gateway IP for the orchestrator on the configuration network.

Step 18 Confirm all of your configuration parameters.

Step 19 Click **Finish**.

After a few minutes, the OVF will be deployed. After the OVA upload completes, you might need to refresh the VMware vSphere GUI session to be able to power on and access the orchestrator virtual machine.

Step 20 If necessary, click the **Refresh** button next to the logged in user name at the top right of the VMware vSphere console.

Step 21 Power on the **orchestrator-1** virtual machine.

Within a few minutes, the IP address that you entered in step 17 begins replying to ping requests.

Step 22 After the orchestrator is up, open a new browser tab and point your browser to the following URL:

```
http://orchestrator-ip:9000/
```

The Setup window opens in your browser.

Note Starting from Secure Workload release 3.8 and later, non-ASCII characters are not allowed to be entered in any of the text fields for site configurations using Secure Workload Setup User Interface.

Step 23 In the Setup window, upload the RPMs in the following order:

a. `rpminstall`

b. `adhoc`

c. `mother`

d. `enforcement` (not applicable for releases earlier than 3.5.1.x)

e. `os_ova`

To upload the RPMs, perform the following substeps:

a) Click **Choose File**.
b) Navigate to an RPM, choose it, and click **Open**.
c) Click **Upload**.
d) Repeat these steps for each RPM.

Step 24 Enter the site information following the standard installation procedure, and see Site Information, on page 6 for hypervisor-specific guidelines.

Step 25 Click **Continue** and follow the standard site installation steps.

After the deployment starts, you will begin to see virtual machines that are created in VMware vSphere in the order of **orchestrator-2** and **orchestrator-3**, then the rest of the Secure Workload stack. If you do not see any virtual machines that were created after 15 minutes, check the deployment logs that are available in the Setup window by clicking the **Details** button.

Step 26 Monitor the Secure Workload setup process, which takes approximately 1.5 hours to complete on hardware that matches the recommended specifications.

After deployment has reached 100%, take note of the virtual IP address that is shown in the status line. If you accidentally close the installer, note the IP address for the virtual IP address. The virtual IP address is the first available IP address that was provided to the installer.

Step 27 Open a tab page in your browser and point the browser to the GUI fully qualified domain name (FQDN) that you entered in the site information section.

Step 28 Click **Forgot Password?**.

Step 29 Enter the email address that you entered for the site administrator and click **Send password reset link**.

Step 30 Check your inbox for the email and follow the included instructions.

If necessary, check your **Spam** folder.

Step 31 Configure anti-affinity rules for certain VM roles that provide redundancy within the Secure Workload infrastructure. Anti-affinity rules must be put in place for instances of the following base types:

- orchestrator
- adhoc
- appServer
- collectorDatamover
- datanode
- druidCoordinator
- druidHistoricalBroker
- elasticsearch
- enforcementCoordinator
- enforcementPolicyStore
- happobat
- hbaseMaster
- hbaseRegionServer
- launcherHost
- mongodb
- namenode and secondaryNamenode
- redis
- tsdbBosunGrafana
- zookeeper

Step 32 In the **VMware VM** configuration screen, right-click **orchestrator-1** and choose **Edit Settings**.

Step 33 Click the **Virtual Hardware** tab.

Step 34 For **Network Adapter 3**, deselect the **Connected** box.

Step 35 Click **OK** to apply the changes.

Failure to remove the checkmark from the **Connected** box can leave the cluster exposed to other configurations after the installation process has completed.

Licensing

Clusters on this platform are restricted to a 30-day trial license when deployed. After 30 days, the cluster will stop processing new data, but the user interface and data collected and processed when the cluster was active will still be accessible. To avoid service disruption, you must apply valid licensing before the evaluation period expires. For more information, see the online help/user guide in the Cisco Secure Workload web portal.

Administrative Guidelines for Commission/Decommission

When using the commission/decommission feature for Secure Workload Virtual environments, please observe the following important guidelines:

- This feature is meant to be used only with the assistance of Cisco TAC, and can cause unrecoverable damage if used incorrectly. No two VMs should ever be decommissioned at the same time, without explicit approval from TAC. The following combinations of VMs must never be decommissioned concurrently:
  - More than one Orchestrator
  - More than one datanode
  - More than one namenode (namenode or secondaryNamenode)
  - More than one resourceManager
  - More than one happobat
  - More than one mongodb (mongodb or mongoArbiter)
- Only one decommission/commission process can be executed at a time. Do not overlap the decommission/commission process for different VMs at the same time.
- Please always contact Cisco TAC prior to using the esx_commission snapshot endpoint.