Tenable and VMware Integration Guide

Last Revised: October 18, 2024

Table of Contents

Welcome to VMware

This document provides information and steps for integrating Tenable Vulnerability Management, Tenable Nessus, or Tenable Security Center with VMware. For more information, refer to the following product documentation:

- Tenable Nessus
- Tenable Security Center
- Tenable Vulnerability Management

Virtualization environments include a combination of hypervisors, management servers, often a large number of virtual machines, and can be complicated. Integrating Tenable Vulnerability Management, Tenable Security Center, or Tenable Nessus with VMware allows you to scan these environments for a comprehensive cyber exposure view.

The VMware integration collects information from vCenter servers, ESXi servers, or a combination of both. You can integrate with VMware by listing VMware ESXi and/or vCenter servers as scan targets. Additional functionality is available when enabling credentialed scans, using the **VMware vCenter API** and **VMware ESX SOAP API** credentials for the respective hosts. Credentialed scans also make it possible to scan for compliance.

What information does the integration collect?

> **Note:** Tenable's VMware integrations support both IPv4 and IPv6 environments.

ESXi and vCenter Versions

The majority of VMware vulnerability checks are based on the versions of ESXi and/or vCenter. Scans collect the versions of both ESXi and vCenter servers in the target list through an unauthenticated API call.

In the case where a vCenter server manages one or more ESXi servers, ESXi version information can also be obtained from the vCenter server (for example, in the event that ESXi servers are not routable from the scanner). This requires successful authentication to the vCenter server.

VMware Installation Bundles

In addition to ESXi and vSphere version information, credentialed scans collect VMware Installation Bundles (VIBs). Collecting VIBs requires successful authentication to vCenter or ESXi, and in the case of vCenter it also requires Lifecycle Manager permissions. For more on required permissions, see the section on required permissions. VIBs are stored in the scanner's Knowledge Base (KB).

The successful collection of VIBs is the criteria for which an ESXi host may have the value of "credentialed checks" set to "yes." If setting up a credential for vCenter or ESXi hosts, you must be able to list VIBs.

Auto-Discovery of ESXi Hosts and Virtual Machines

Credentialed scans can enumerate the ESXi hosts and virtual machines and add them as targets to be scanned. For more, see the section on auto-discovery.

Compliance

Tenable Vulnerability Management, Tenable Security Center, or Tenable Nessus can scan VMware environments for compliance. Compliance checks are targeted, credentialed checks of ESXi and/or vCenter servers based on the targets listed in the settings.

When scanning a vCenter host, Tenable reports about the vCenter server and any ESXi servers that the vCenter manages. When scanning an ESXi host, the scan reports about the ESXi host. It is possible to scan both ESXi and vCenter hosts in a single scan.

Compliance checks use the SOAP API, unlike normal vulnerability checks which use the REST API for VMware versions 7.0.3 and newer.

> **Note:** Compliance scanning is unavailable with the Auto-Discovery feature enabled.

What the VMware integration does not collect

The VMware integration does not collect information about the vCenter or ESXi host operating systems. Additionally, the VMware integration cannot collect all information about virtual machines themselves (for example, operating system details).

> **Note:** You can configure additional SSH or Windows credentials for the vCenter and/or ESXi hosts in order to scan for operating system vulnerabilities.

Note: You can configure additional SSH or Windows credentials for virtual machines discovered using the integration in order to scan for operating system vulnerabilities.

For more information about each product integration, see VMware in the Tenable Nessus, Tenable Vulnerability Management, and Tenable Security Center user guides.

Configure VMware ESX SOAP API

Required Permissions

The ESX SOAP API credential uses the VMware ESXi SOAP API. The ESX credential requires a user account with read-only permissions or a user account with administrator level permissions.

The following steps detail how to create a read-only user with the minimum privilege level required:

1. Log into ESXi.
2. (Optional) If necessary, create a new user account.
    a. Under **Navigator**, expand the **Host** category and select **Manage**.
    b. In the **Manage** window, select **Users**, then click **Add user**.
    c. Add a user with the desired username and password.
3. Under **Navigator**, select **Host**.

    A new window opens.
4. Click **Actions**.
5. Under **Actions**, select **Permissions**.

    The **Manage permissions** window appears.
6. Select the user you want to use as a read-only user, then click **assign role**.
7. Select **Propagate to all children**.
8. Click **Assign role**.
9. Run a Tenable scan to verify the permissions worked.

You should expect to see the scan showing not only vulnerabilities, but that credentialed checks are enabled on the ESXi host.

Note: Some compliance audits, specifically those with "Bare Metal" in the name, require an SSH credential to be configured. Configuring these audits displays a notice that SSH credentials are required. When configuring an SSH credential to an ESXi server, the user must be an administrator-level user. The read-only user cannot be used. This only applies to the SSH users required by these "Bare Metal" audits.

Scan Configuration

Access to VMware servers is available through its native SOAP API. VMware ESX SOAP API allows you to access the ESX and ESXi servers via username and password. Also, you have the option of not enabling SSL certificate verification:

For more information on configuring the VMWare ESX SOAP API, see Configure vSphere Scanning.

VMware can access VMware ESXi servers through the native VMware SOAP API.

Option	Description	Default
Username	(Required) The username for the ESXi server account that Tenable uses to perform checks on the target system	-
Password	(Required) The password for the ESXi user.	-
Do not verify SSL Certificate	Do not validate the SSL certificate for the ESXi server.	Disabled

VMware ESX SOAP API Helpful Guidelines

VMware ESXi SOAP API Scan Results Review

This section provides the user resources to review scan results from the plugin output and debug log reporting in an effort to help guide you in the scan results review process for the vCenter Integration.

Plugin Families and Plugins

Settings

Nessus Scan Information (19506) - Credentialed Checks

Tenable has observed user confusion with respect to **Credentialed Checks: 'yes/no**' in plugin ID 19506 (Nessus Scan Information) and how authentication is interpreted with the vCenter integration. Unless an SSH credential is included along with a VMware vCenter SOAP API credential, credentialed checks do not represent a failed/successful authentication to the host. What is the difference? Traditionally, when running an authenticated scan to a host using SSH or Windows credentials, you can expect to see **Credential Checks: 'yes/no'** based on whether login credentials to the target machine were valid. In the case of the VMware ESXi SOAP API integration, Tenable is authenticating to the ESXi SOAP API, not the host machine, which is an important difference to highlight.

When running a scan using the VMware ESXi SOAP API integration, you can expect to see Credentialed Checks:

- 'yes' if the integration collected VIBs for that host and Credentialed Checks:
- 'no' if the integration did not collect VIBs.

Service Detection

VMware vSphere Detect (57396)

This plugin gathers the ESXi version from an unauthenticated SOAP API call to the ESXi host. The version gathered from this plugin is used for ESXi vulnerability detection plugins that rely on versioning. This plugin runs independently of the integration and it is not indicative of ESXi authentication issues experienced using the integration.

VMware ESX Local Security Checks

VMware vSphere Installed VIBs (57400)

This plugin reports the installed VIBs collected on a ESXi host. Other plugins and processes are dependent on the successful collection of ESXi installed VIBs, such as Credentialed Checks and

vulnerability detection plugins. However, Tenable does not execute vulnerability detections on specific VIBs data collected.

VMware Active Virtual Machines (57397)

This plugin reports active virtual machines (powered on) that were collected on a specific ESXi host and therefore are reported on the applicable ESXi host.

VMware Inactive Virtual Machines (57398)

This plugin reports inactive virtual machines (powered off) that were collected on a specific ESXi host and therefore are reported on the applicable ESXi host.

> **Note:** In addition to these integration-related plugins, ESXi vulnerability detection plugins belong to the VMware ESXi Local Security Checks plugin family. If this plugin family is disabled, scan results will not include these vulnerability detections.

Policy Compliance

VMware vCenter/vSphere Compliance Checks (64455)

This plugin must be enabled in order to execute compliance scanning and performs compliance checks against ESXi hosts. This plugin is automatically enabled if an audit file that requires it is added to the scan.

Plugin Debug Log Reporting

Unlike the vCenter integration, plugin debugging is not centralized in a collection. It consists of individual plugins that generate logs for VIBs and Active/Inactive virtual machines. When troubleshooting, remember that ESXi SOAP API authentication occurs in each of these.

ESXi Installed VIBs: vmware_installed_vibs.log
ESXi Active Virtual Machines: vmware_active_vms.log
ESXi Inactive Virtual Machines: vmware_inactive_vms.log
vmware_compliance_check.log
vmware_compliance_check_debug.log

> **Note:** Do not refer to the vmware_vsphere_detect.log for authentication-related concerns. Tenable sends an unauthenticated SOAP API call to the ESXi host to retrieve the version. The logs in this file can be misleading and do not represent authentication success or failure.

When running a scan using the VMware ESXi SOAP API Integration, you can expect to see Credentialed Checks:

- ‘yes’ if the integration collected VIBs for that host and Credentialed Checks:
- ‘no’ if the integration did not collect VIBs.

Configure VMware vCenter API

This credential supports versions containing SOAP and REST APIs. Tenable automatically chooses which API to use based on the vCenter/ESXi version detected. The SOAP API is used for versions less than 7.0.3 and the REST API is used for version 7.0.3 or later.

> **Note:** Tenable does not support the use of mixed version environments where the REST API is not available on some hosts. For example, vCenter 7.0.3 managing ESXi server versions less than 7.0.3. is not supported, but vCenter 8 managing ESXi server version 7.0.3 is supported.

Required Permissions

A scan configured with the vCenter credential uses the REST API for vulnerability checks against versions 7.0.3+ and the SOAP API for versions less than 7.0.3.

> **Note:** In a compliance scan, regardless of version, the scan uses the SOAP API to collect configuration information at the level of detail required for compliance auditing.

When using the vCenter credential for vulnerability scanning, the scanner makes the following REST API requests to the vCenter server:

- POST /api/session (log in)
- GET /api/vcenter/host
- GET /api/ESX/hosts/<host>/software/installed-components

The following steps detail how to create a read-only user with the minimum privilege level required:

1. Log into vCenter.
2. (Optional) If necessary, create a new user account.
    a. Under **Administration** > **Access Control**, select **Roles**.
    b. Create a new role with any name you prefer (for example, "Nessus").
3. Select the **VMware vSphere Lifecycle Manager** category.

    A new window opens.
4. Under **Lifecycle Manager: Image Privileges** select **Read**.
5. (Optional) If you wish to perform compliance scans, select the following additional privilege: **Global -> Settings**.
6. Click **Create** to create the “Nessus” role.
7. Go to the **Inventory** page.
8. Right-click the root vCenter Object at the top of the left-hand tree.

    A new menu opens.
9. Click **Add Permission**.
10. Select the user account, and select the "Nessus" role.
11. Select the **propagate to children** checkbox, then click **OK**.
12. Run a Tenable Scan to verify permissions work.
13. For additional troubleshooting, see the troubleshooting section.

Resources

VMware documentation on the REST API endpoints that the vCenter integration uses:

- GET /api/vcenter/host
- GET /api/ESX/hosts/<host>/software/installed-components

Scan Type	API Type	Permissions Needed
vCenter credential for	REST	Lifecycle Manager:

vulnerability scanning		Image Privileges = Read
ESXi hosts using ESXi credentials	SOAP	User = Read Only
Compliance Scan	SOAP	Global -> Settings

Scan Configuration

For more information on configuring the VMWare vCenter SOAP API, see Configure vSphere Scanning.

VMware can access vCenter through the native VMware vCenter SOAP API. If available, Tenable Nessus uses the vCenter REST API to collect data on versions 7.0.3+ and uses the SOAP API on versions less than 7.0.3.

Credential: VMware vCenter SOAP API

Option	Description
vCenter Host	(Required) The name of the vCenter host.
vCenter Port	(Required) The TCP port that vCenter listens on for communications from Tenable.
Username	(Required) The username for the vCenter server account with admin read/write access that Tenable uses to perform checks on the target system.
Password	(Required) The password for the vCenter server user.
HTTPS	When enabled, Tenable connects using secure communication (HTTPS).

	When disabled, Tenable connects using standard HTTP.
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA. If you are using a self-signed certificate, disable this setting.
Auto Discover Managed VMware ESXi Hosts	This option adds any discovered VMware ESXi hypervisor hosts to the scan targets you include in your scan.
Auto Discover Managed VMware ESXi Virtual Machines	This option adds any discovered VMware ESXi hypervisor virtual machines to the scan targets you include in your scan.

Credential: VMware vCenter API

Option	Description
vCenter Host	(Required) The name of the vCenter host.
vCenter Port	(Required) The TCP port that vCenter listens on for communications from Tenable.
HTTPS	When enabled, Tenable connects using secure

	communication (HTTPS). When disabled, Tenable connects using standard HTTP.
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA. If you are using a self-signed certificate, disable this setting.
VMware vCenter API Authentication Method	(Required) The user can choose from a list of authentication methods: • Username and Password (manual entry) • PAM Integration (use a specific PAM to gather vCenter API Authentication Credentials from the available list)
Auto Discover Managed VMware ESXi Hosts	This option adds any discovered VMware ESXi hypervisor hosts to the scan targets you include in your scan.
Auto Discover Managed VMware ESXi Virtual Machines	This option adds any discovered VMware ESXi hypervisor virtual machines

	to the scan targets you include in your scan.

VMware vCenter API Helpful Guidelines

REST API Endpoints

There are a number of API endpoints that the integration makes requests to. This document focuses on the REST API endpoints that are supported on vCenter 7.0.3 and above.

Tenable is asked a lot about permissions. In the most simplistic way, you must have permissions configured to get a successful response back from the following API endpoints. It is critical that when performing the following tests that they be run from the scanner to rule out any network connectivity issues with the vCenter Host. While running them from any machine is valid, this rules out the scanner's ability/inability to communicate with the vCenter Host.

The following curl commands contain environmental variables (e.g., `${VCENTER_USERNAME}`. If you are not familiar with the use of environmental variables then using manual entry within the commands is another option. Options are provided for both in each section.

vCenter API Authentication

Tenable uses bearer token authentication authorized to the vCenter username/password entered in the scan credentials.

Users can use this simple curl command test to ensure this user has the appropriate permissions and to rule out any authentication issues to the vCenter REST API before running a scan.

Users can choose to export environmental variables, such as VCENTER_USERNAME. The following list of curl commands is formatted for environmental variables. Users can also manually enter these values. If executed manually, an example of the `username:password` of the authentication command would look like this:

`-u "myuser:mypassword"`

```
curl -k -X POST -u "${VCENTER_USERNAME}:${VCENTER_PASSWORD}"
https://${VCENTER}/api/session
```

Manual entry option:

Replace `"${VCENTER_USERNAME}:${VCENTER_PASSWORD}"` with `-u "myuser:mypassword"`

Replace `${VCENTER}` with your vCenter IP address or FQDN

A successful response yields a session token that can be used for subsequent requests. Example of a successful response, which is the session token to be used in subsequent requests: "7b08862e67aa48f758c627fc2aa710a6"

If the user does not obtain a session token, here are some possible reasons why:

Reason: Incorrect Username and/or Password
Status Code 401: Unauthorized
Server Response:

```
{
  "error_type": "UNAUTHENTICATED",
  "messages": [
    {
      "args": [],
      "default_message": "Authentication required.",
      "id": "com.vmware.vapi.endpoint.method.authentication.required"
    }
  ]
}
```

Reason: Incorrect vCenter Host, vCenter Host does not support REST API, or tried to verify SSL certificate in a scan policy.
Status Code 500: Server Error
Server Response: Error 500 Server Error or no response at all

Get a list of ESXi hosts managed by vCenter

If authentication to the vCenter REST API was successful, Tenable then makes a request to vCenter to gather a list of ESXi hosts that it manages. This list of ESXi hosts are enumerated in subsequent requests.

To test this, the user can run the following curl command:

```
curl -k -X GET -H "vmware-api-session-id: ${SESSION}"
https://${VCENTER}/api/vcenter/host
```

Manual entry option:

Replace `${SESSION}` with the value received from the authentication request.

Replace `${VCENTER}` with your vCenter IP address or FQDN

If successful, users can expect the following response.

Status Code 200: OK
Server Response:


```
[
  {
    "host": "host-1006",
    "name": "1.1.1.1",
    "connection_state": "CONNECTED",
    "power_state": "POWERED_ON"
  },
  {
    "host": "host-1007",
    "name": "1.1.1.2",
    "connection_state": "CONNECTED",
    "power_state": "POWERED_ON"
  },
  {
    "host": "host-1008",
    "name": "1.1.1.3",
    "connection_state": "CONNECTED",
    "power_state": "POWERED_ON"
  }
]
```


Get a list of installed software components (VIBs) per ESXi host:

In this request, Tenable asks vCenter to report on the installed software components (VIBs) for each of the ESXi hosts that it manages. The user takes the “host” (host-id) for any of the list of hosts from the previous call and test the following command to rule out any permission errors.

User

```
curl -k -X GET -H "vmware-api-session-id: ${SESSION}"
https://${VCENTER}/api/esx/hosts/${ESX_HOST}/software/installed-components
```

The ${ESX_HOST} value should be the one of the “host” values received from the request to get a list of ESXi hosts managed by the vCenter

Manual entry option:

Replace ${SESSION} with the value received from the authentication request.

Replace ${VCENTER} with your vCenter IP address or FQDN

Replace ${ESX_HOST} with one of the “host” values received from the request to get a list of ESXi hosts managed by the vCenter.

A successful response would yield similar results.

Status Code 200: OK
Server Response:


```
{
  "Broadcom-ELX-IMA-plugin": {
    "display_version": "12.0.1200.0-6vmw",
    "display_name": "Broadcom IMA plugin for Emulex OneConnect iSCSI Driver",
    "version": "12.0.1200.0-6vmw.800.1.0.20513097",
    "platforms": [
      "host"
    ]
  },
  "Broadcom-ELX-brcmfcoe": {
    "display_version": "12.0.1500.3-4vmw",
    "display_name": "Broadcom Emulex Connectivity Division fcoe driver for FCoE
adapters",
    "version": "12.0.1500.3-4vmw.800.1.0.20513097",
    "platforms": [
      "host"
    ]
  },
  "Broadcom-ELX-lpfc": {
```

```
    "display_version": "14.0.635.4-14vmw",
    "display_name": "Broadcom Emulex Connectivity Division lpfc driver for FC
adapters",
    "version": "14.0.635.4-14vmw.800.1.20.21203435",
    "platforms": [
      "host"
    ]
  },
  "esx-update": {
    "display_version": "8.0.0 Build 21493926",
    "display_name": "ESXi Install/Upgrade Component",
    "version": "8.0.0-1.25.21493926",
    "platforms": [
      "host"
    ]
  },
  "esxio-update": {
    "display_version": "8.0.0 Build 21493926",
    "display_name": "ESXi Install/Upgrade Component",
    "version": "8.0.0-1.25.21493926",
    "platforms": [
      "host"
    ]
  }
}
```


Most often, if the user does not have the correct vCenter Lifecycle Manager permissions, they receive the following response. Refer to our permissions section for proper configuration.

Status Code 403: UNAUTHORIZED
Server Response:


```
{
  "error_type": "NOT_FOUND",
  "messages": [
    {
      "args": [],
      "default_message": "Not found.",
      "id": "com.vmware.vapi.rest.httpNotFound."
```

```
    }
  ]
}
```

Get a list of virtual machines per ESXi host

Tenable sends a request to the vCenter API to get a list of virtual machines hosted on a specific ESXi. This list of virtual machines is enumerated in subsequent requests.

```
curl -f -k -X GET -H "vmware-api-session-id: ${SESSION}"
https://${VCENTER}/api/vcenter/vm?hosts=${ESX_HOST}
```

Manual entry option:

Replace `${SESSION}` with the value received from the authentication request.

Replace `${VCENTER}` with your vCenter IP address or FQDN

Replace `${ESX_HOST}` with one of the “host” values received from the request to get a list of ESXi hosts managed by the vCenter.

Get virtual machine details for a specific virtual machine

From the list of virtual machines, you can take one of the virtual machine IDs (e.g., vm-1024) and send a request to vCenter to retrieve virtual machine details for that specific virtual machine.

The `${VM}` value should be the one of the “vm” values received from the request to get a list of virtual machines hosted on the ESXi server.

```
curl -f -k -X GET -H "vmware-api-session-id: ${SESSION}"
https://${VCENTER}/api/vcenter/vm/${VM}/guest/identity
```

Manual entry option:

Replace `${SESSION}` with the value received from the authentication request.

Replace `${VCENTER}` with your vCenter IP address or FQDN

Replace `${VM}` with one of the “vm” values received from the request to get a list of virtual machines hosted on the ESXI server.

If a VM is powered off, this results in a status code of `503 Service Unavailable`. If this happens, users can run the following alternative command.

```
curl -f -k -X GET -H "vmware-api-session-id: ${SESSION}"
https://${VCENTER}/api/vcenter/vm/${VM}
```

Manual entry option:

Replace `${SESSION}` with the value received from the authentication request.

Replace `${VCENTER}` with your vCenter IP address or FQDN

Replace `${VM}` with one of the “vm” values received from the request to get a list of virtual machines hosted on the ESXi server.

VMware vCenter API Scan Results Review

This section explains scan results from plugin output to debug log reporting in an effort to help guide you in the review process for the vCenter Integration.

Plugin Families and Plugins

General

Integration Discovered Host (168417)

Reports on targets that were added to the scan using an auto-discovery feature in an integration. vCenter is a Tenable integration that supports auto-discovery, specifically ESXi, and virtual machine hosts.

Settings

Nessus Scan Information (19506) - Credentialed Checks

Tenable has observed user confusion with respect to Credentialed Checks: ‘yes/no’ in plugin ID 19506 (Nessus Scan Information) and how authentication is interpreted with the vCenter integration. Unless an SSH credential is included along with a VMware vCenter SOAP API credential, Credentialed Checks do not represent failed/successful authentication to the host. What is the difference? Traditionally, when running an authenticated scan to a host using SSH or Windows credentials, users can expect to see Credentialed Checks: ‘yes/’no’ based on whether login credentials to the target machine were valid. In the case of the vCenter Integration, Tenable is

authenticating to the vCenter API, not the host machine, so this is an important difference to point out.

When running a scan using the VMware ESXi SOAP API Integration, you can expect to see Credentialed Checks:

- 'yes' if the integration collected VIBs for that host and Credentialed Checks:
- 'no' if the integration did not collect VIBs.

Tenable plans to release a new plugin in 2024 to signal success/failure of authentication and other requests to various vCenter API endpoints, in order to clear up confusion and make this simple for users. In the meantime, refer to the troubleshooting tips in the following sections for help with diagnosing potential errors that may arise.

Service Detection

VMware vCenter Detect (63061)

This plugin gathers the vCenter version from an unauthenticated SOAP API call to the vCenter host. It's important to note that even later versions (v7.0.3) maintain a SOAP API. The version gathered from this plugin is used for vCenter vulnerability detection plugins that rely on versioning. This plugin runs independently of the integration and it is not indicative of vCenter authentication issues experienced using the integration. However, it does serve a purpose when deciding whether to collect vCenter and ESXi host data from either the vCenter SOAP or REST API, which is version-dependent; SOAP less than v7.0.3 and REST v7.0.3+.

VMware vSphere Detect (57396)

This plugin gathers the ESXi version from an unauthenticated SOAP API call to the ESXi host. The version gathered from this plugin is used for ESXi vulnerability detection plugins that rely on versioning. This plugin runs independently of the integration and it is not indicative of vCenter authentication issues experienced using the integration.

VMware ESX Local Security Checks

VMware vCenter Data Collection (63062)

This plugin handles everything from authentication to the vCenter REST API, collection of vCenter managed ESXi hosts, collection of ESXi VIBs, ESXi managed virtual machines, and virtual machine details for vCenter and ESXi versions 7.0.3+. You can find additional information related to the

debug log for this plugin in the Debug Log Reporting section of this document. Data collection and storage is executed on only one of the targets in the target settings and is used for reporting on subsequent targets enumerated during the scan.

VMware vCenter Legacy Data Collection (180178)

This plugin executes everything from authentication to the vCenter SOAP API, collection of vCenter managed ESXi hosts, collection of ESXi VIBs, ESXi managed virtual machines, and virtual machine details for vCenter and ESXi versions less than 7.0.3. You can find additional information related to the debug log for this plugin in the Debug Log Reporting section of this document. Data collection and storage is executed on only one of the targets in the target settings and is used for reporting on subsequent targets enumerated during the scan.

VMware vCenter Auto-Discovery (180179)

This plugin executes the auto-discovery process when the user has enabled Auto-Discovery of ESXi hosts and virtual machines. You can find additional information related to the debug log for this plugin in the Debug Log Reporting section of this document.

VMware vCenter Managed ESXi Installed VIBs (154017)

This plugin reports the installed VIBs collected on a vCenter managed ESXi host. Other plugins and processes are dependent on the successful collection of ESXi installed VIBs, such as Credentialed Checks and vulnerability detection plugins. However, Tenable does not execute vulnerability detections on the specific VIBs data collected.

VMware vCenter Active Virtual Machines (84340)

This plugin reports active virtual machines (powered on) that were collected on a specific ESXi host and therefore are reported on the applicable ESXi host.

VMware vCenter Inactive Virtual Machines (84341)

This plugin reports inactive virtual machines (powered off) that were collected on a specific ESXi host and therefore are reported on the applicable ESXi host.

> **Note:** In addition to these integration-related plugins, ESXi vulnerability detection plugins belong to the VMware ESXi Local Security Checks plugin family. If this plugin family is disabled, scan results will not include these vulnerability detections.

Policy Compliance

VMware vCenter/vSphere Compliance Checks (64455)

This plugin must be enabled in order to execute compliance scanning and perform compliance checks against both vCenter and ESXi hosts.

Plugin Debug Log Reporting

vCenter Authentication and Data Collection

When troubleshooting or verifying authentication to the vCenter API, users can find this debug log reporting in `vmware_vcenter_collect.nbin~Collection_host` for REST (v7.0.3+) and `vmware_vcenter_collect_legacy.nbin~Collection_host` for SOAP (less than v7.0.3). `Collection_host` is presented by the IP/FQDN of the host that the collection was executed on, which is done only once. In verifying successful vCenter authentication, it is important to look in the correct debug logs. Specifically, do not verify authentication by looking in the debug logs for the VMware vCenter Detect or VMware vSphere detect plugins. These detection plugins are unrelated to the integration and should not be used to verify authentication, because they always perform unauthenticated requests.

These logs also contain all other aspects of data collection including retrieving all ESXi hosts managed by a vCenter, VIBs installed for each ESXi, virtual machines hosted on ESXi, and virtual machine details for each virtual machine.

For example, if a particular ESXi host in the scan results has credentialed checks: no, the user should already know that there are potentially a few issues that could cause this from happening:

- Authentication to the vCenter API failed, therefore no data was retrieved.
- It is possible that this particular host was not retrieved as a managed ESXi host on the vCenter host in the credential, therefore VIBs were not retrieved.
- The ESXi host is managed by vCenter, but there was an error in the response to the request to collect VIBs for that particular host.

The user can look at this collection log and see if any issues were encountered. With the help of the curl tests provided in the REST API Endpoints section, Tenable has given the user some resources to help diagnose their issues with the integration.

Auto-Discovery Feature

You can enable Auto-Discovery of ESXi hosts managed by a vCenter and/or virtual machines hosted on ESXi hosts managed by a vCenter. Instead of manually entering in ESXi Hosts and virtual machines in the target settings, enablement of the Auto-Discovery option automatically adds to a scan; all ESXi hosts discovered on the vCenter and, if enabled, virtual machines hosted on each discovered ESXi host.

Note: This feature is only available when scanning vCenter/ESXi versions 7.0.3 and above.

Note: Auto-Discovery does not automatically add the ability to authenticate remotely to ESXi hosts and virtual machines. You can add additional SSH credentials to authenticate to the ESXi host discovered and added to the scan, as well as SSH/Windows credentials to authenticate to virtual machines discovered and added to the scan.

Why would you prefer Auto-Discovery over manual entry of ESXi and virtual machine targets?

- This is especially convenient for users with large volumes of ESXi hosts and virtual machines who want to scan the entire environment. Tenable removes the need to “know before you go” and reduces time in scan creation and preparation.
- Some users have their ESXi hosts configured behind a firewall, or simply do not allow any incoming traffic. The manual entry method does not work in this case because the scanner cannot communicate with the host. An additional capability of the Auto-Discovery feature allows these particular ESXi hosts to “live” in the scan. At minimum, this allows VIBs reporting on each ESXi host and vulnerability plugins related to version checks to execute. Here is a Tenable Community post with additional details of this capability.