Tenable and Nutanix Integration Guide

Last Revised: January 08, 2025

Table of Contents

Welcome to Nutanix

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

- Tenable Nessus Manager
- 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 Nutanix Prism Central allows you to scan these environments for a comprehensive cyber exposure view.

Tenable's integration with Nutanix Prism Central API allows for the collection and enumeration of virtual environments during scans to collect host software versions, assisting with patch management and vulnerability detection.

How it works

Through the use of one of Tenable's products (Tenable Vulnerability Management or Tenable Security Center), users can configure a Nutanix Prism Central credential under Miscellaneous credential types. This credential policy is then sent to the internally linked scanner to communicate with the Nutanix Prism Central API host. Tenable authenticates to the API based on the values provided in the scan credential and collect a variety of data.

What information does the Nutanix Prism Central integration collect?

Tenable attempts to collect data with respect to all hypervisors and virtual machines managed by the Nutanix central host. This information includes clusters, nodes, IP addresses, host software versions, services, and architecture. Data collected allows for scanning the Nutanix AOS and AHV products for known host vulnerabilities.

What the Nutanix Prism Central integration does not collect

The Nutanix Prism Central integration does not collect information about the collected host operating systems. Additionally, the Nutanix Prism Central integration can not collect all information about virtual machines themselves (for example, operating system details). At no point is Tenable authenticating to hosts discovered during the collection process. Tenable only authenticates to the API of the Prism Central host. The traditional concept of “Credentialed Checks” in Nessus Scan Information (Nessus Plugin ID 19506) does not apply here.

Note: Users can configure additional SSH or Windows credentials for the Controller VM (CVM) and hypervisors in order to scan for operating system vulnerabilities.

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

Scan Configuration

Option	Description	Default
Nutanix Host	(Required) The name of the Nutanix Prism Central host.	-
Nutanix Port	(Required) The port for the Nutanix Prism Central host.	9440
Username	(Required) The username for the Nutanix Prism Central account.	-
Password	(Required) The password for the Nutanix Prism Central user.	-
Discover Hosts	When enabled, Tenable Security Center adds all discovered Nutanix hosts to the list of scan targets.	enabled
Discover Virtual Machines	When enabled. Tenable Security Center adds all discovered Nutanix Virtual Machines to the list of scan targets.	enabled
HTTPS	When enabled, Tenable connects using secure communication (HTTPS). When disabled, Tenable connects using standard HTTP.	enabled
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA. **Tip:** If you are using a self-signed certificate, disable this setting.	disabled

Helpful Guidelines

Determining Success of the Integration

Nutanix Data Collection (Plugin ID 160185)

If data collection was successful, this plugin reports a variety of data collected on the target through the API. In the event this plugin does not report, you can run an audit trail on the host and plugin ID.

Integration Status (Plugin ID 204872)

This plugin reports success or failure based on Tenable's attempt to gather cluster information.

Additional Logs

In the event that you encounter integration failure, if debug log reporting is enabled (Tenable recommends level 3 or 4) you can review the `nutanix_collect.nasl~Nutanix Prism Central` log to troubleshoot issues like authentication failure, HTTP error codes from API responses, and custom log messages with helpful pointers.

Advanced Troubleshooting

Tenable requests data from three different Nutanix Prism Central API resources. Following are a set of curl commands, either of which you can run to help troubleshoot potential problems. Tenable recommends running these from the terminal that hosts the scanner.

Collecting Cluster Data

Data collected from Nutanix Prism Central integration from this cluster resource is used for vulnerability detections. Replace the `ip_address`, `username`, and `password` variables with your own data:

```
curl -kv --request POST \
    --url https://ip_address:9440/api/nutanix/v3/clusters/list \
    --header 'Accept: application/json' \
    -u 'username:password' \
    --header 'Content-Type: application/json' \
    --data '{
    "kind": "cluster",
    "length": 1,
    "offset": 0,
    "sort_attribute": "uuid",
    "sort_order": "ASCENDING"
}'
```

A successful response contains the following schema, which goes into great detail regarding the cluster list of hosts and details in the `entities` attribute.

```
{
  "api_version": "3.1",
  "metadata": {...},
  "entities": [
    {...}
  ]
}
```

If a connection is established with the web server and you encounter errors, the following schema is shown with the HTTP error code and detailed messaging. Otherwise, the -v flag is added in the curl command for verbosity to expose curl errors which can be troubleshooted with a simple web search.

```
{
  "kind": "cluster",
  "code": 0,
  "message_list": [
    {...}
   ],
  "state": "string",
  "api_version": "3.1.0"
}
```

Collecting Hypervisors and VMs using Auto Discovery (Optional)

Tenable provides the options to discover hypervisors and/or virtual machines during a scan and automatically add them as targets to be scanned against. This is less likely to be a troubleshooting avenue, but to be thorough, here are commands that can be run. The schema for success and error responses from the API are identical to the cluster request above.

Collecting Hypervisors

```
curl -kv --request POST \
    --url https://ip_address:9440/api/nutanix/v3/hosts/list \
    --header 'Accept: application/json' \
    -u 'username:password' \
    --header 'Content-Type: application/json' \
    --data '{
    "kind": "host",
    "length": 1,
    "offset": 0,
    "sort_attribute": "uuid",
    "sort_order": "ASCENDING"
}'
```

Collecting Virtual Machines

```
curl -kv --request POST \
    --url https://ip_address:9440/api/nutanix/v3/vms/list \
    --header 'Accept: application/json' \
    -u 'username:password' \
    --header 'Content-Type: application/json' \
    --data '{
    "kind": "vm",
    "length": 1,
    "offset": 0,
    "sort_attribute": "uuid",
    "sort_order": "ASCENDING"
}'
```