Setup Integration from Qualys

Qualys Vulnerability Management, Detection and Response (VMDR)

This Qualys VMDR (external, opens in a new tab or window) integration is a cloud-based service that gives you immediate, global visibility into where your IT systems might be vulnerable to the latest Internet threats and how to protect them. It helps you to continuously identify threats and monitor unexpected changes in your network before they turn into breaches.

The Qualys VMDR integration uses REST API mode to collect data. Elastic Agent fetches data via API endpoints.

Compatibility

This module has been tested against the latest Qualys VMDR version **v2**.

Data streams

The Qualys VMDR integration collects data for the following three events:

Event Type
Asset Host Detection
Knowledge Base
User Activity Log

Starting from Qualys VMDR integration version 6.0, the Asset Host Detection data stream includes enriched vulnerabilities data from Qualys Knowledge Base API.

- https://docs.qualys.com/en/vm/latest/

Requirements

- Elastic Agent must be installed.

- You can install only one Elastic Agent per host.
- Elastic Agent is required to stream data through the REST API and ship the data to Elastic, where the events will then be processed via the integration's ingest pipelines.

Agentless Enabled Integration

Agentless integrations allow you to collect data without having to manage Elastic Agent in your cloud. They make manual agent deployment unnecessary, so you can focus on your data instead of the agent that collects it. For more information, refer to Agentless integrations (external, opens in a new tab or window) and the Agentless integrations FAQ (external, opens in a new tab or window). Agentless deployments are only supported in Elastic Serverless and Elastic Cloud environments. This functionality is in beta and is subject to change. Beta features are not subject to the support SLA of official GA features.

- https://www.elastic.co/docs/solutions/security/get-started/agentless-integrations
- https://www.elastic.co/docs/troubleshoot/security/agentless-integrations

Installing and managing an Elastic Agent:

You have a few options for installing and managing an Elastic Agent:

Install a Fleet-managed Elastic Agent (recommended):

With this approach, you install Elastic Agent and use Fleet in Kibana to define, configure, and manage your agents in a central location. We recommend using Fleet management because it makes the management and upgrade of your agents considerably easier.

Install Elastic Agent in standalone mode (advanced users):

With this approach, you install Elastic Agent and manually configure the agent locally on the system where it’s installed. You are responsible for managing and upgrading the agents. This approach is reserved for advanced users only.

Install Elastic Agent in a containerized environment:

You can run Elastic Agent inside a container, either with Fleet Server or standalone. Docker images for all versions of Elastic Agent are available from the Elastic Docker registry, and we provide deployment manifests for running on Kubernetes.

There are some minimum requirements for running Elastic Agent and for more information, refer to the link here.

- https://www.elastic.co/docs/reference/fleet/install-elastic-agents

Description:

Integrate Qualys Vulnerability Management, Detection and Response (VMDR) with the Elastic Stack using REST API-based methods. This allows you to ingest vulnerability, asset, and detection data directly into Elasticsearch for centralized security monitoring, visualization, and analysis.

What It Does:

- Connects to Qualys VMDR using the REST API
- Fetches vulnerability data, asset inventory, and host-level detections
- Enables structured indexing, Kibana dashboards, and Elastic SIEM correlation
- Supports both manual script-based integration and automated Elastic Agent setup

Option 1: API-Based Script Integration

Description:

Use Qualys' REST API with a custom script (e.g., Python) to pull data and send it to Elasticsearch.

What It Does:

- Fetches Qualys scan results, vulnerabilities, and asset data on demand
- Allows you to customize scheduling, parsing, and indexing behavior
- Works with any self-managed Elastic cluster or Elastic Cloud deployment

Steps:

Prepare API Access:

- Log in to Qualys Admin Portal → User Management
- Create a dedicated API user with:
  - API Access permission
  - Access to VMDR, Host, and Detection modules
- Save the username and password for authentication

Call the API:

```
GET https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/
```

Use Basic Authentication with your API user credentials.

Python Example Script:

```
import requests, json
from requests.auth import HTTPBasicAuth
response = requests.get(
    "https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/",
    auth=HTTPBasicAuth("QUALYS_USER", "PASSWORD"),
    headers={"X-Requested-With": "curl"}
)
data = {"raw_data": response.text}
requests.post(
    "http://<elasticsearch>:9200/qualys-vulns/_doc",
    headers={"Content-Type": "application/json"},
    data=json.dumps(data)
)
```

Option 2: Elastic Agent – Qualys VMDR Integration (REST API)

Description:

Use Elastic Agent’s built-in **Qualys VMDR integration** to automatically fetch vulnerability and asset data via the REST API and ingest it directly into Elasticsearch.

What It Does:

- Connects to Qualys VMDR using a dedicated API user
- Fetches data streams like detections, vulnerabilities, and host asset inventory
- Provides ready-made Kibana dashboards and works with Elastic Security rules
- Fully managed through Fleet UI in Elastic Cloud or self-managed Elastic Stack

Steps:

Enable API Access in Qualys:

- Ensure a Qualys API user exists
- Grant the following:
    - API Access
    - Access to VMDR, Host, Detection, and Inventory modules as needed

Install Elastic Agent:

- Install Elastic Agent on your server, endpoint, or VM
- Enroll it into Fleet via Kibana or Elastic Cloud

Add the Qualys VMDR Integration:

- Go to **Kibana → Fleet → Integrations**
- Search for **“Qualys VMDR”** and click **Add Integration**
- Enter:
    - API Server URL (e.g., `https://qualysapi.qualys.com`)
    - API Username
    - API Password
    - Optional: page size or polling interval

Choose Data Streams to Collect:

- `vulnerability`
- `detection`
- `host`
- `asset_inventory` (if supported)

Save the Integration Policy:

- Attach the policy to an Elastic Agent
- Agent will start fetching and shipping data automatically

References:

- *https://www.elastic.co/docs/reference/integrations/qualys_vmdr*
- *https://cdn2.qualys.com/docs/qualys-api-vmpc-user-guide.pdf*

> “
> ## What Happens Next

When you run your custom script (Option 1):
→ Data is pulled from Qualys via REST API and posted to a target Elasticsearch index
→ You control the fetch frequency, field mappings, and transformation logic
→ Dashboards must be manually built or customized in Kibana

When you enable Elastic Agent integration (Option 2):
→ Agent continuously pulls vulnerability and detection data from Qualys
→ Prebuilt dashboards populate in Kibana
→ Vulnerabilities can be used in SIEM detection rules or custom queries

Integration Requirements Overview

Component	Required for Option 1 (Script)	Required for Option 2 (Elastic Agent)	Purpose
Qualys API User	Yes	Yes	Authenticates to Qualys for REST API access
VMDR Module Access	Yes	Yes	Needed to access host, detection, and vulnerability data
Role-Based Access Control (RBAC)	Yes	Yes	Ensures the API user only accesses required modules
Custom Script	Yes	No	Required only for manual API integration
Elastic Agent	No	Yes	Required for Fleet-managed automatic integration
Kibana Access	Yes	Yes	Used to view dashboards and run security queries

Permissions

Asset Host Detection

Role	Permission
Managers	All VM scanned hosts in subscription
Unit Managers	VM scanned hosts in user’s business unit
Scanners	VM scanned hosts in user’s account
Readers	VM scanned hosts in user’s account

Knowledge Base

Managers, *Unit Managers*, *Scanners*, *Readers* have permission to download vulnerability data from the KnowledgeBase.

User Activity Log

Role	Permission
Managers	All actions taken by all users

Role	Permission
Unit Managers	Actions taken by users in their business unit
Scanners	Own actions only
Readers	Own actions only

Setup

To collect data through REST API, follow the below steps:

- Considering you already have a Qualys user account, to identify your Qualys platform and get the API URL, refer this link.
  - https://www.qualys.com/platform-identification/
- Alternative way to get the API URL is to log in to your Qualys account and go to Help > About. You’ll find your URL under Security Operations Center (SOC).

Enabling the integration in Elastic:

1. In Kibana go to Management > Integrations
2. In "Search for integrations" search bar, type Qualys VMDR
3. Click on the "Qualys VMDR" integration from the search results.
4. Click on the Add Qualys VMDR Integration button to add the integration.
5. While adding the integration, if you want to collect Asset Host Detection data via REST API, then you have to put the following details:
   - username
   - password
   - url
   - interval
   - input parameters
   - batch size

   or if you want to collect Knowledge Base data via REST API, then you have to put the following details:
   - username
   - password
   - url
   - initial interval
   - interval
   - input parameters

   or if you want to collect User Activity log data via REST API, then you have to put the following details:
   - username
   - password
   - url
   - initial interval
   - interval

Screenshot

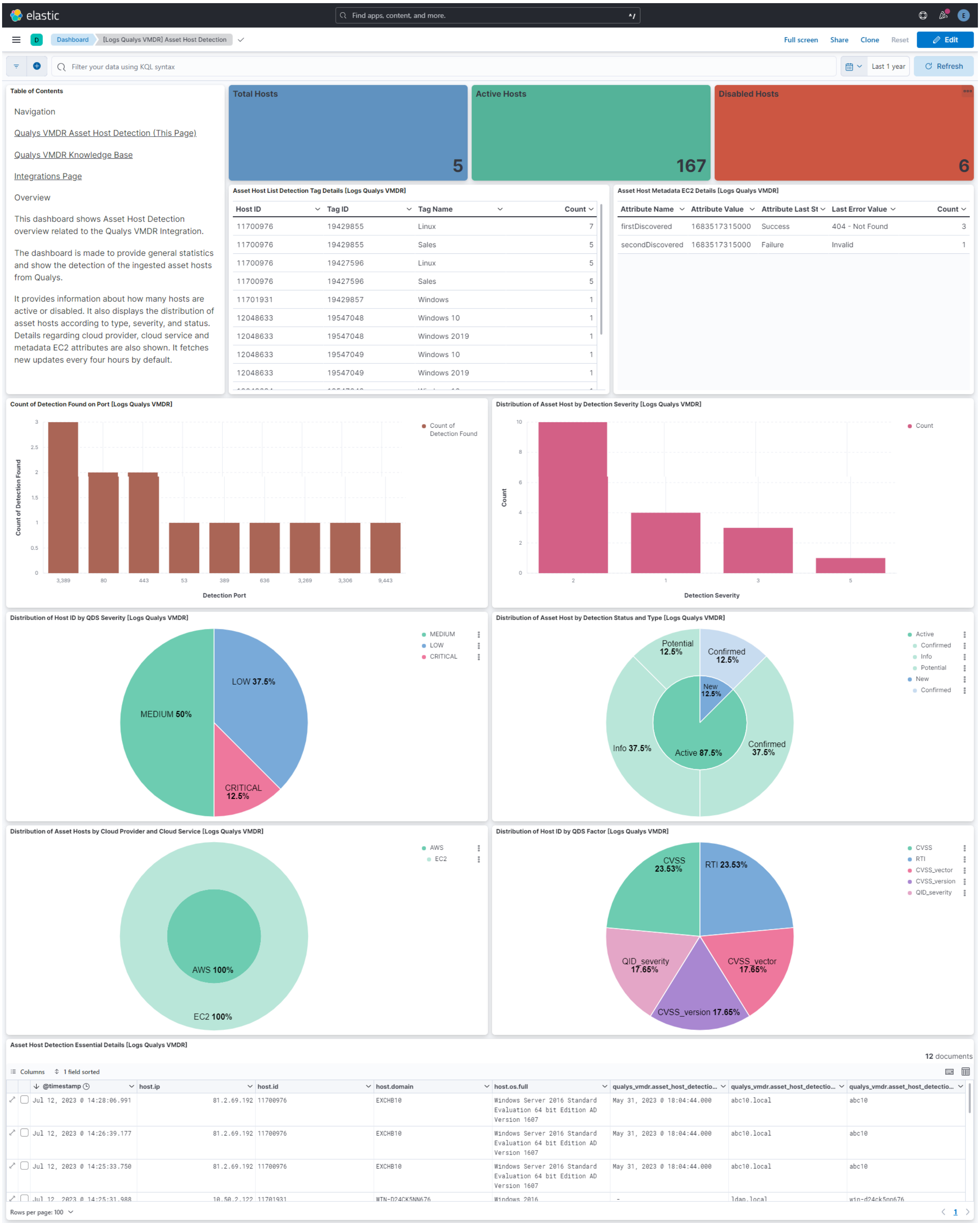
elastic
Find apps, content, and more.
Dashboard
[Logs Qualys VMDR] Asset Host Detection
Full screen
Share
Clone
Reset
Edit
Filter your data using KQL syntax
Last 1 year
Refresh

Table of Contents

Navigation

Qualys VMDR Asset Host Detection (This Page)

Qualys VMDR Knowledge Base

Integrations Page

Overview

This dashboard shows Asset Host Detection overview related to the Qualys VMDR Integration.

The dashboard is made to provide general statistics and show the detection of the ingested asset hosts from Qualys.

It provides information about how many hosts are active or disabled. It also displays the distribution of asset hosts according to type, severity, and status. Details regarding cloud provider, cloud service and metadata EC2 attributes are also shown. It fetches new updates every four hours by default.

Total Hosts 5

Active Hosts 167

Disabled Hosts 6

Asset Host List Detection Tag Details [Logs Qualys VMDR]

Host ID	Tag ID	Tag Name	Count
11700976	19429855	Linux	7
11700976	19429855	Sales	5
11700976	19427596	Linux	5
11700976	19427596	Sales	5
11701931	19429857	Windows	1
12048633	19547048	Windows 10	1
12048633	19547048	Windows 2019	1
12048633	19547049	Windows 10	1
12048633	19547049	Windows 2019	1

Asset Host Metadata EC2 Details [Logs Qualys VMDR]

Attribute Name	Attribute Value	Attribute Last St	Last Error Value	Count
firstDiscovered	1683517315000	Success	404 - Not Found	3
secondDiscovered	1683517315000	Failure	Invalid	1

Count of Detection Found on Port [Logs Qualys VMDR]

Distribution of Asset Host by Detection Severity [Logs Qualys VMDR]

Distribution of Host ID by QDS Severity [Logs Qualys VMDR]

Distribution of Asset Host by Detection Status and Type [Logs Qualys VMDR]

Distribution of Asset Hosts by Cloud Provider and Cloud Service [Logs Qualys VMDR]

Distribution of Host ID by QDS Factor [Logs Qualys VMDR]

Asset Host Detection Essential Details [Logs Qualys VMDR]

12 documents

@timestamp	host.ip	host.id	host.domain	host.os.full	qualys_vmdr.asset_host_detectio...	qualys_vmdr.asset_host_detectio...	qualys_vmdr.asset_host_detectio...
Jul 12, 2023 @ 14:28:06.991	81.2.69.192	11700976	EXCHB10	Windows Server 2016 Standard Evaluation 64 bit Edition AD Version 1607	May 31, 2023 @ 18:04:44.000	abc10.local	abc10
Jul 12, 2023 @ 14:26:39.177	81.2.69.192	11700976	EXCHB10	Windows Server 2016 Standard Evaluation 64 bit Edition AD Version 1607	May 31, 2023 @ 18:04:44.000	abc10.local	abc10
Jul 12, 2023 @ 14:25:33.750	81.2.69.192	11700976	EXCHB10	Windows Server 2016 Standard Evaluation 64 bit Edition AD Version 1607	May 31, 2023 @ 18:04:44.000	abc10.local	abc10
Jul 12, 2023 @ 14:25:31.988	10.50.2.122	11701931	WIN-D24CK5NN676	Windows 2016	-	ldap.local	win-d24ck5nn676

Revision #3
Created 19 June 2025 07:26:59 by Kent Lauron
Updated 20 June 2025 01:33:21 by Kent Lauron