Nutanix Data Lens

Last updated: Jun. 24, 2025

Overview

Nutanix Data Lens is a SaaS-based data security solution offering ransomware resilience and intelligent analytics for unstructured data on Nutanix Cloud Platform (NCP). This service offers global data visibility to proactively assess and mitigate data security risks by identifying anomalous activity, auditing user behavior, and adhering to compliance requirements, while enabling efficient data lifecycle management.

Nutanix alert & event log types ingested by this data connector:

- Licensing
- Capacity
- Security
- Configuration

Requirements

CrowdStrike subscription: Falcon Next-Gen SIEM or Falcon Next-Gen SIEM 10GB.

CrowdStrike clouds: Available in US-1, US-2, EU-1, and US-GOV-1.

CrowdStrike access and permissions: Administrator or Connector Manager access to the Falcon console for the respective CID.

Vendor requirements

- Nutanix Data Lens license
- Administrator role in Nutanix Data Lens

Setup

> **Important:** Some of these steps are performed in third-party products. CrowdStrike does not validate any third-party configurations in customer environments. Perform the following steps with care, and validate your settings and values before finalizing configurations in the Falcon console.

Step 1: Configure and activate the Nutanix Data Lens Data Connector

1. In the Falcon console, go to Data connectors > Data connectors > Data connections [/data-connectors].
2. Click **+ Add connection**.
3. In the **Data Connectors** page, filter or sort by **Connector name**, **Vendor**, **Product**, **Connector Type**, **Author**, or **Subscription** to find and select the connector you want to configure.

   > **Tip:** This data connector's name is located in the header. For example, **Step 1: Configure and activate** `<the_data_connector_name>`.

4. In **New connection**, review connector metadata, version, and description. Click **Configure**.

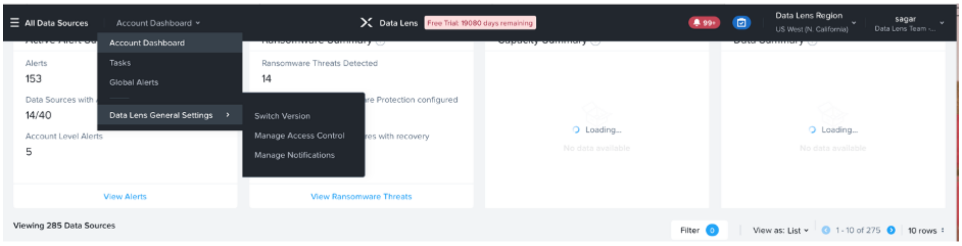
   > **Note:** For connectors that are in a **Pre-production** state, a warning appears. Click **Accept** to continue configuration.

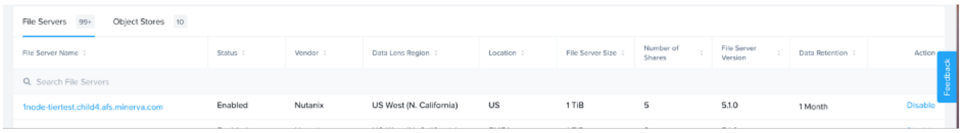
5. In the **Add new connector** page, enter a name and optional description to identify the connector.
6. Click the **Terms and Conditions** box, then click **Save**.
7. A banner message appears in the Falcon console when your API key and API URL are ready to be generated. To generate the API key, go to Data connectors > Data connectors > Data connections [/data-connectors], click **Open menu** ⋮ for the data connector, and click **Generate API key**.
8. Copy and safely store the API key and API URL to use during connector configuration.

   > **Important:** Record your API key somewhere safe as it displays only once during connector setup. For more information about vendor-specific connector setup, see the Third-party data source integration guides [/documentation/page/a76b8289/data-connectors#c42a73ec].

Step 2: Configure the API key and API URL in Nutanix Data Lens

1. Go to **Account Dashboard > Data Lens General Settings > Manage Notifications.**

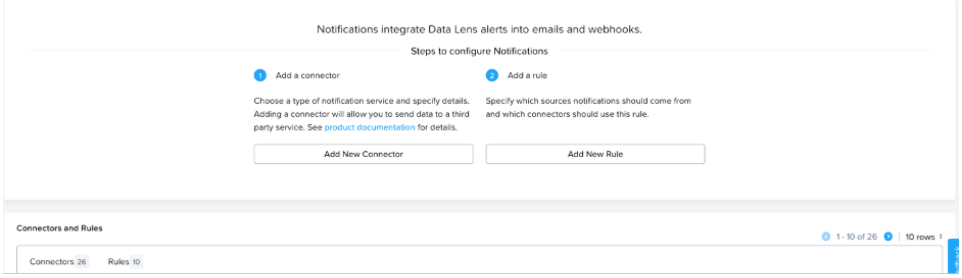




File Servers 99+ Object Stores 10

File Server Name	Status	Vendor	Data Lens Region	Location	File Server Size	Number of Shares	File Server Version	Data Retention	Action
Search File Servers									
1node-tiertest.child4.afs.minerva.com	Enabled	Nutanix	US West (N. California)	US	1 TiB	5	5.1.0	1 Month	Disable

2. On the **Notifications** page, click **Add New Connector**.



Notifications integrate Data Lens alerts into emails and webhooks.

Steps to configure Notifications

1 Add a connector

Choose a type of notification service and specify details. Adding a connector will allow you to send data to a third party service. See product documentation for details.

2 Add a rule

Specify which sources notifications should come from and which connectors should use this rule.

Connectors and Rules

1 - 10 of 26 | 10 rows

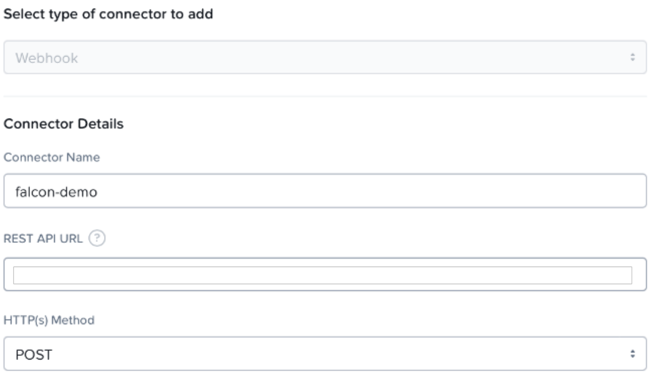
Connectors 26 Rules 10

3. Enter the connector details:

   a. **Connector Name:** Enter a name for this connector.

   b. **Rest API URL:** Add the API URL you saved in Step 1: Configure and activate the Nutanix Data Lens Data Connector [/documentation/page/q81d11d8/nutanix-data-lens#x82dc3b8].

   c. **HTTP(s) Method**: Make sure the **POST** method is selected.



Select type of connector to add

Webhook

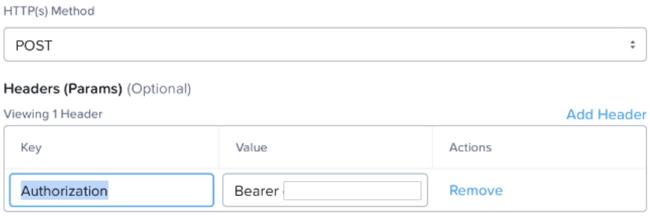
Connector Details

Connector Name: falcon-demo

REST API URL:

HTTP(s) Method: POST

   d. **Headers (Params)**: For **Key**, type in Authorization. For **Value**, type in Bearer. After Bearer, paste the API key you saved in step 1. For example, `Bearer ef4c400112f3456789`.



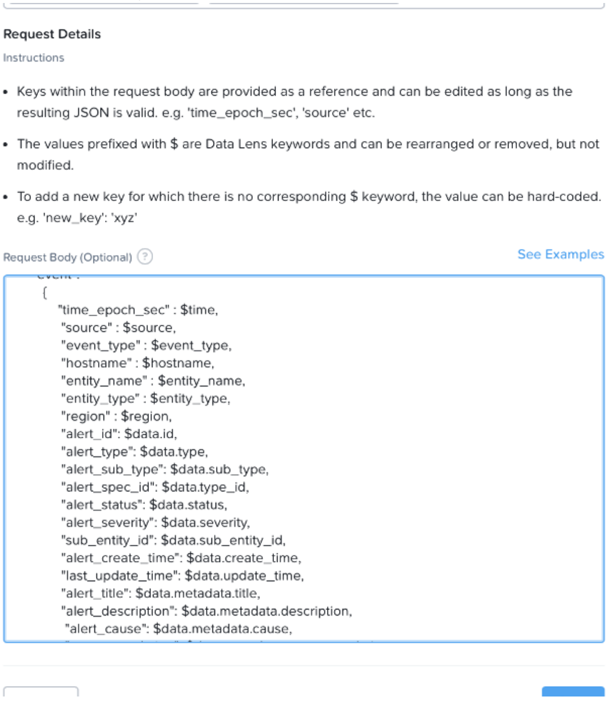
HTTP(s) Method: POST

Headers (Params) (Optional)

Viewing 1 Header

Key	Value	Actions
Authorization	Bearer	Remove

   e. In the **Request Details** section, add the following JSON example to the **Request Body** box.



Request Details

Instructions

- Keys within the request body are provided as a reference and can be edited as long as the resulting JSON is valid. e.g. 'time_epoch_sec', 'source' etc.
- The values prefixed with $ are Data Lens keywords and can be rearranged or removed, but not modified.
- To add a new key for which there is no corresponding $ keyword, the value can be hard-coded. e.g. 'new_key': 'xyz'

Request Body (Optional)

```
  {
    "time_epoch_sec" : $time,
     "source" : $source,
     "event_type" : $event_type,
     "hostname" : $hostname,
     "entity_name" : $entity_name,
     "entity_type" : $entity_type,
     "region" : $region,
     "alert_id": $data.id,
     "alert_type": $data.type,
     "alert_sub_type": $data.sub_type,
     "alert_spec_id": $data.type_id,
     "alert_status": $data.status,
     "alert_severity": $data.severity,
     "sub_entity_id": $data.sub_entity_id,
     "alert_create_time": $data.create_time,
     "last_update_time": $data.update_time,
     "alert_title": $data.metadata.title,
     "alert_description": $data.metadata.description,
      "alert_cause": $data.metadata.cause,
```

f. Click **Save**.

4. Go to **Account Dashboard > Data Lens General Settings > Manage Notifications.** Select **Add New Rule**.

5. Configure a rule to use with the connector you just created:

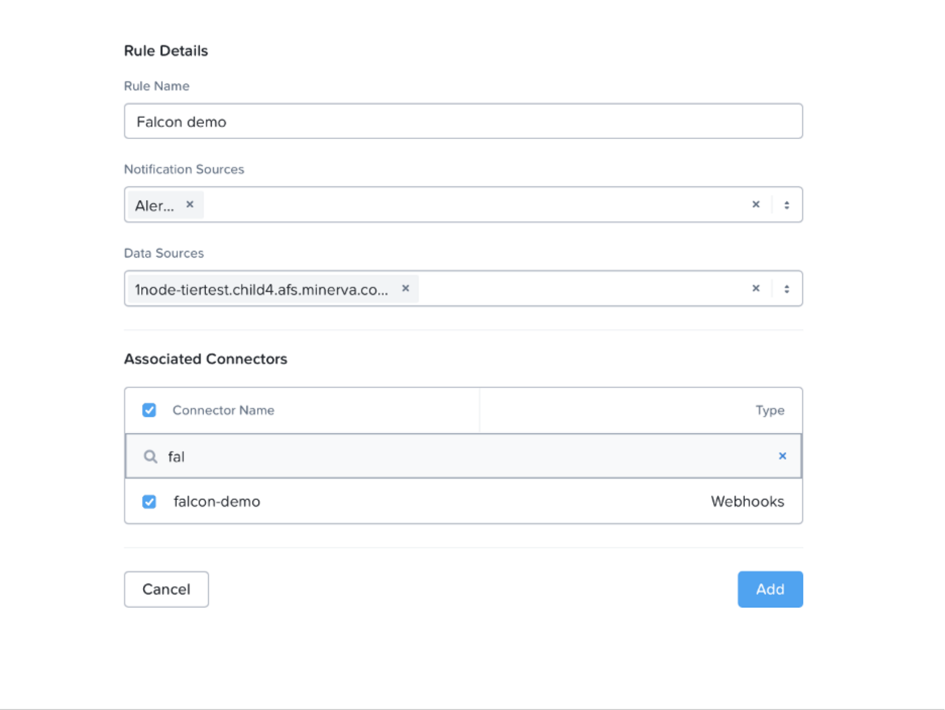
   a. **Name:** Enter a name for the rule.

   b. **Notification Sources:** Choose which notification sources you want notifications from. For more info, see Nutanix Data Lens Alerts and Notifications [https://portal.nutanix.com/page/documents/solutions/details?targetId=TN-2188-Nutanix-Data-Lens:nutanix-data-lens-alerts-and-notifications.html]
   .

   c. **Data Sources:** Choose a data source. If you want notifications from all data sources, select the **All** checkbox.

   d. **Associated Connectors:** Click the checkbox for the connector you just created.

   e. Click **Add**.



Rule Details

Rule Name: Falcon demo

Notification Sources: Aler... ×

Data Sources: 1node-tiertest.child4.afs.minerva.co... ×

Associated Connectors

☑ Connector Name	Type
fal	
☑ falcon-demo	Webhooks

Step 3: Verify successful data ingestion

> **Important:** Search results aren't generated until an applicable event occurs. Before verifying successful data ingestion, wait until data connector status is **Active** and an event has occurred. Note that if an event timestamp is greater than the retention period, the data is not visible in search.

Verify that data is being ingested and appears in Next-Gen SIEM search results:

1. In the Falcon console, go to **Data connectors > Data connectors > Data connections [/data-connectors]**.

2. In the **Status** column, verify data connection status is **Active**.

3. In the **Actions** column, click **Open** menu ⋮ and select **Show events** to see all events related to this data connection in **Advanced Event Search**.

4. Confirm that at least one match is generated.

If you need to run a manual search, use this query in Advanced Event Search:

```
#Vendor = "nutanix" | #repo = "3pi_nutanix_data_lens" | #event.module = datalens
```

Data reference

Parser

The default parser recommended to parse incoming data for this data connector is **nutanix-datalens**.

Supported timestamp format: `yyyy-MM-dd HH:mm:ss.SSSSSSxxx`

Example: `2024-12-11 00:17:21.151000+00:00`

Structure

Expected log structure

```
{
        "alert_cause": "S3 replication bucket Config Validation failed",
        "sub_entity_id": "",
        "alert_status": "Open",
        "alert_sub_type": "S3Analytics",
        "alert_create_time": "2024-10-23 22:51:28.554000+00:00",
        "recommendation": "Please look into the recommendations in S3 Analytics account update email.",
        "alert_spec_id": "s3_replication_bucket_config_validation_failed",
        "alert_type": "Application",
        "last_update_time": "2024-10-23 22:51:28.554000+00:00",
        "alert_description": "While running periodic sub_entity_discovery job for S3 Analytics config
validation failed for bucket associated with cloud vendor 834650 and Nutanix account: 293452169.",
        "alert_title": "S3 replication bucket config validation failed",
        "alert_id": "2bedba2c-0abe-46b7-b978-65d3f252ab5d",
        "alert_severity": "1"
    }
```

Next-Gen SIEM events

Next-Gen SIEM events that can be generated by this data connector:

- Vulnerability:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#j7b1c38l]
- Iam:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#e3wbhf1h]
- Threat:Indicator:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#s455fd5m]
- Configuration:Access:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#w71kufuj]
- Configuration:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#e1mjpydj]
- Iam:User:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#u8x1u9jm]
- Host:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#w5nxhce9]

For more information about Next-Gen SIEM events, see Next-Gen SIEM Data Reference [/documentation/page/q1f14b54/next-gen-siem-data] .

‹ Nasuni Edge Events[/documentation/page/l30d7037/nasuni]

Obsidian Security › [/documentation/page/w38a6fa1/obsidian-security-data-connector]