

Jumpcloud Integrations

Introduction

The JumpCloud integration allows you to monitor events related to the JumpCloud Directory as a Service via the Directory Insights API.

You can find out more about JumpCloud and JumpCloud Directory Insights here

- <https://jumpcloud.com/platform/directory-insights>

Data streams

A single data stream named "jumpcloud.events" is used by this integration.

Assumptions

The procedures described in Section 3 assumes that a Log Collector has already been setup.

Requirements

An Elastic Stack with an Elastic Agent is a fundamental requirement.

An established JumpCloud tenancy with active users is the the other requirement. Basic Directory Insights API access is available to all subscription levels.

NOTE: The lowest level of subscription currently has retention limits, with access to Directory Insights events for the last 15 days at most. Other subscriptions levels provide 90 days or longer historical event access.

A JumpCloud API key is required, the JumpCloud documentation describing how to create one is here

- <https://support.jumpcloud.com/s/article/jumpcloud-apis1>

This JumpCloud Directory Insights API is documented here

- <https://docs.jumpcloud.com/api/insights/directory/1.0/index.html#section/Overview>

JumpCloud Integration Procedures

Procedures:

Please provide the following information to CyTech:

Enabling the integration in Elastic

1. In Kibana go to Management > Integrations
2. In "Search for integrations" search bar type JumpCloud
3. Click on "JumpCloud" integration from the search results.
4. Click on Add JumpCloud button to add the JumpCloud integration.
5. Configure the integration as appropriate
6. Assign the integration to a new Elastic Agent host, or an existing Elastic Agent host

[< Cancel](#)

Add JumpCloud integration

Configure an integration for the selected agent policy.

1 Configure integration

Integration settings

Choose a name and description to help identify how this integration will be used.

Integration name

Description

Optional

[> Advanced options](#)

Poll Directory Insights API for Events

[Change defaults ^](#) JumpCloud Directory Insights API

Beta

Collect JumpCloud Events via JumpCloud Directory Insights API

URL of JumpCloud Directory Insights API endpoint

i.e. scheme://host:port/path

JumpCloud Directory Insights API Key

Preserve original event

Preserves a raw copy of the original event, added to the field event.original

[> Advanced options](#)

2 Where to add this integration?

[New hosts](#) Existing hosts

Create agent policy

Add this integration to a new set of hosts by creating a new agent policy. You can add agent in the next step.

New agent policy name

 Collect system logs and metrics ⓘ[> Advanced options](#)[Cancel](#) [Preview API request](#)[Save and continue](#)

Revision #2

Created 23 April 2024 13:33:31

Updated 19 June 2024 06:54:01