



Cloud Insights documentation

Cloud Insights

NetApp

April 04, 2023

Table of Contents

Cloud Insights documentation	1
What can Cloud Insights do for me?	1
Getting Started	1
What's New with Cloud Insights	2
March 2023	2
January 2023	2
December 2022	2
November 2022	4
October 2022	4
September 2022	5
August 2022	6
June 2022	11
May 2022	14
April 2022	16
March 2022	18
February 2022	19
December 2021	20
November 2021	22
October 2021	23
September 2021	25
August 2021	26
June 2021	27
May 2021	30
April 2021	31
February 2021	34
January 2021	35
December 2020	37
November 2020	38
October 2020	39
September 2020	39
August 2020	41
July 2020	41
June 2020	49
May 2020	50
April 2020	53
February 2020	55
January 2020	56
December 2019	58
November 2019	58
October 2019	59
September 2019	59
August 2019	61
July 2019	61

June 2019	62
May 2019	62
April 2019	63
March 2019	63
February 2019	64
January 2019	64
December 2018	64
November 2018	65
Cloud Insights Onboarding	66
Creating your NetApp Cloud Central account	66
Starting your Cloud Insights free trial	66
Sign in and go	66
Logging Out	67
Security	68
Cloud Insights Security	68
Information and Region	70
Getting Started	73
Feature Tutorials	73
Collecting Data	74
Importing from the Dashboard Gallery	121
User Accounts and Roles	122
Cloud Insights Data Collector List	130
Subscribing to Cloud Insights	134
Editions	134
Trial Version	135
Trial through AWS Marketplace	135
Subscription Options	136
How Do I Subscribe?	137
View Your Subscription Status	138
View your Usage Management	138
Subscribe Directly and Skip the Trial	139
Adding an Entitlement ID	139
Automatic Device Resolution	140
Automatic Device Resolution Overview	140
Device Resolution rules	142
Fibre Channel device resolution	145
IP device resolution	147
Setting options in the Preferences tab	149
Regular expression examples	150
Creating Dashboards	157
Dashboards Overview	157
Dashboard Features	160
Sample Dashboards	191
Best Practices for Dashboards and Widgets	196
Kubernetes Explorer	201

Kubernetes Cluster Overview	201
Kubernetes Cluster Detail Page	202
ONTAP Essentials	207
Overview	207
Data Protection	208
Alerts	208
Infrastructure	209
Networking	210
Workloads	210
Working with Queries	212
Assets used in queries	212
Creating Queries	213
Viewing queries	218
Exporting query results to a .CSV file	218
Modifying or Deleting a Query	219
Assigning multiple applications to or removing multiple applications from assets	220
Copying table values	221
Log Explorer	221
Working with Annotations	225
Defining annotations	225
Using annotations	227
Creating annotation rules	230
Importing Annotations	231
Working with Applications	234
Tracking asset usage by application	234
Creating Applications	234
Monitors and Alerts	236
Alerting with Monitors	236
Viewing and Managing Alerts from Monitors	245
Configuring Email Notifications	247
System Monitors	248
Cloud Insights API	314
Requirements for API Access	314
API Documentation (Swagger)	314
API Access Tokens	315
API Type	316
Inventory Traversal	316
Expands	317
Performance Data	319
Object Performance Metrics	321
Performance History Data	321
Objects with Capacity Attributes	322
Using Search to Look Up Objects	323
Disabling or Revoking an API Token	323
Rotating Expired API Access Tokens	324

Notification using Webhooks	326
Creating a Webhook	326
Choosing Webhook Notification in a Monitor	329
Webhook Examples:	329
Monitoring your Environment	330
Auditing	330
Asset Page Information	333
Asset Page Overview	333
Filtering for Objects In-Context	334
Asset Page Summary section	335
Expert View	337
User Data Section	342
Asset Page Related Alerts section	343
Configuring an LDAP Directory Server Collector	350
User Management	354
SVM Event Rate Checker (Agent Sizing Guide)	354
Alerts	359
Alert	359
Filter Options	360
The Alert Details page	361
<i>Take a Snapshot Action</i>	362
Alert Notifications	363
Retention Policy	363
Troubleshooting	364
Forensics	365
Forensics - All Activity	365
Forensic Entities Page	369
Forensic User Overview	371
Automated Response Policies	372
Integration with ONTAP Autonomous Ransomware Protection	374
Prerequisites	374
User permissions required	374
Sample Alert	375
Limitations	376
Troubleshooting	376
Blocking User Access	377
Prerequisites for User Access Blocking	377
How to enable the feature?	377
How to set up Automatic user access blocking?	378
How to know if there are blocked users in the system?	378
Restrict and manage user access manually	378
User Access Limitation History	378
How to disable the feature?	378
Manually Restore IPs for NFS	378
Manually Restore Users for SMB	379

Troubleshooting	380
Workload Security: Simulating an Attack	382
Things to note before you begin	382
Have at least 1,000 sample files	382
Guidelines before you run the simulator:	382
Prepare the system	382
Run the Ransomware Simulator script	383
Encrypt your test files	383
Restore files	384
Run the script multiple times	384
Create files programmatically	384
Configuring Email Notifications for Alerts, Warnings, and Agent/Data Source Collector health	386
Potential Attack Alerts and Warnings	386
Agent and Data Collector Health monitoring	386
Workload Security API	387
API Documentation (Swagger)	387
API Access Tokens	387
Active IQ	389
Opening the Active IQ page	390
Querying for Risks	391
Dashboards	392
Troubleshooting	393
Troubleshooting General Cloud Insights Problems	394
Login issues:	394
Troubleshooting Acquisition Unit Problems on Linux	396
Considerations about Proxies and Firewalls	398
Resources	399
Troubleshooting Acquisition Unit Problems on Windows	400
Considerations about Proxies and Firewalls	401
Resources	402
Researching a failed data collector	403
Reference & Support	404
Requesting Support	405
Activating support entitlement	405
Obtaining Support Information	408
Cloud Insights Data Collector Support Matrix	410
Cloud Insights Data Collector Support Matrix	411
Data Collector Reference - Infrastructure	412
Vendor-Specific Reference	412
Configuring the Amazon EC2 data collector	412
Amazon FSx for NetApp ONTAP data collector	415
Configuring the Azure compute data collector	417
Broadcom	419
Cisco MDS Fabric Switches data collector	422
Cohesity SmartFiles data collector	425

Dell	426
Dell EMC	427
Fujitsu Eternus data collector	451
NetApp Google Compute data collector	452
HP Enterprise	453
Hitachi Data Systems	461
Infinidat InfiniBox data collector	469
Huawei OceanStor data collector	470
IBM	472
Lenovo data collector	480
Microsoft	481
NetApp	484
Nutanix NX data collector	507
OpenStack data collector	508
Oracle ZFS Storage Appliance data collector	510
Pure Storage FlashArray data collector	512
Red Hat Virtualization data collector	513
Rubrik CDM Data Collector	514
Configuring the VMware VSphere data collector	515
Data Collector Reference - Services	518
Node Data Collection	518
ActiveMQ Data Collector	520
Apache Data Collector	523
Consul Data Collector	526
Couchbase Data Collector	527
CouchDB Data Collector	529
Docker Data Collector	531
Elasticsearch Data Collector	539
Flink Data Collector	543
Hadoop Data Collector	550
HAProxy Data Collector	560
JVM Data Collector	567
Kafka Data Collector	571
Kibana Data Collector	576
Memcached Data Collector	578
MongoDB Data Collector	581
MySQL Data Collector	583
Netstat Data Collector	588
Nginx Data Collector	589
PostgreSQL Data Collector	592
Puppet Agent Data Collector	594
Redis Data Collector	596
Object Icon Reference	599
Legal notices	600
Copyright	601

Trademarks	602
Patents	603
Privacy policy	604
Open source	605

Cloud Insights documentation

NetApp Cloud Insights is a cloud infrastructure monitoring tool that gives you visibility into your complete infrastructure. With Cloud Insights, you can monitor, troubleshoot and optimize all your resources including your public clouds and your private data centers.

What can Cloud Insights do for me?

Cloud Insights provides hybrid multicloud monitoring, giving you full-stack observability of infrastructure and workloads.

- Data collectors for heterogeneous infrastructure and workloads, including Kubernetes
 - Open Telegraf collector and open APIs for easy integration
 - Comprehensive alerting and notifications
 - Machine learning for intelligent insights
 - Optimize resource utilization
 - Built-in or customizable dashboards with advanced filters to minimize display noise to answer questions
 - Discover the health of your ONTAP storage operations
 - Protect your most valuable business asset – data - from ransomware or data destruction attack
-

Getting Started

- How do I [get started](#) with Cloud Insights?
- I'm signed up. Now what do I do?
[Acquiring Data](#)
[Setting up users](#)
- Awesome! What's Next?
[Preparing Assets: Annotating](#)
[Finding the Assets You Want: Querying](#)
[Seeing the Data You want: Dashboards](#)
[Monitoring and Alerts](#)
[Securing Data](#)
- This is great stuff! I'm ready to [subscribe](#).

What's New with Cloud Insights

NetApp is continually improving and enhancing its products and services. Here are some of the latest features and functionalities available with Cloud Insights.

March 2023

Cloud Connection for ONTAP 9.9+ deprecated

The Cloud Connection for ONTAP 9.9+ data collector is being deprecated. Starting April 4, 2023, Cloud Connection data collectors in your environment will no longer collect data, and will instead present an error when polling. The Cloud Connection data collector will be removed altogether from Cloud Insights in a subsequent update.

Prior to April 4, 2023, it is mandatory to configure a new NetApp ONTAP Data Management Software data collector for any ONTAP systems currently collected by Cloud Connection. [Learn More](#).

January 2023

New Log Monitors

We've added almost two dozen [additional system monitors](#) to alert for broken interconnect links, heartbeat problems, and more. Additionally, three new Data Protection log monitors have been added, to alert on SnapMirror Auto Resync, MetroCluster Mirroring, and FabricPool Mirror Resync changes.

Note that some of these monitors will be *enabled* by default; you must *pause* them if you do not wish to alert on them. Also note that these monitors are not configured to deliver notifications; you must configure notification recipients on these monitors if you want to send alerts via email or webhook.

.CSV Export for all Dashboard Table Widgets

Ensuring accessibility to your data is essential, so we've made .CSV export [] available for all metric queries, dashboard table widgets, and object landing pages, regardless of the type of data (asset or integration) you're querying.

Data customizations like column selection, renaming columns, and unit conversions are also now included in the new export functionality.

December 2022

Explore Ransomware Protection and other security features during Cloud Insights Trial

Starting today, signing up for a new Trial of Cloud Insights allows you to explore Security features such as Ransomware detection and automated user-blocking response policy. If you haven't signed up for your Trial, do it today!

Kubernetes Workloads have their own landing page

Workloads are a key part of your Kubernetes environment, so Cloud Insights now provides landing pages for

those workloads. From here, you can view, explore, and troubleshoot issues that affect your Kubernetes workloads.

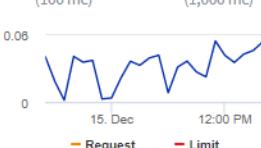
Filter By

1/1 Pods: Current / Desired	- Up-to-date	- Unavailable
---------------------------------------	-----------------	------------------

Namespace dockerimage-monitoring	Type ReplicaSet	Date Created Dec 9, 2022 4:37 PM
Labels -		

54mc
CPU

54% vs. Request (100 mc) 5% vs. Limit (1,000 mc)



Request — Limit

0.22GiB
Memory

44% vs. Request (0.49 GiB) 22% vs. Limit (1.00 GiB)



Request — Limit

0.00GiB
Total PVC Capacity claimed

Highest CPU Demand by Pod

2.8m [telegraf-rs-2xsj2](#)

Highest Memory Demand by Pod

0.21 GiB [telegraf-rs-2xsj2](#)

Pods (1)				
Pod Name ↑	Status	Healthy Containers	cpu_usage_nanocores (mc)	memory_rss_bytes (GiB)
telegraf-rs-2xsj2	● Healthy Running	1 of 1	3	0.21

Check your Checksums

You asked us to provide you with checksum values during installation of the agent for Windows, Linux, and MacOS, and we think that's a great idea. So here they are:

Manually Verifying Telegraf Checksums

The Cloud Insights agent installer performs integrity checks, but some users may want to perform their own verifications before installing or applying downloaded artifacts.

For more information, read about [verifying checksums](#) before proceeding to the next step.

The SHA256 checksum for this telegraf.pkg is:

```
cbd0d8d0512b65fbcd0c786d8d0512b651de0e1cf003e0a0d9df01d8d0512b65
```

Log Alerting Improvements

Group By

When creating or editing a Log Monitor, you can now set "Group By" attributes to allow for more focused alerting. Look for the "Group By" attributes below the "filter" settings in your monitor definition.

1 Select the log to monitor

The screenshot shows a log monitoring interface with the following configuration:

- Log Source:** logs.netapp.ems
- Filter By:** ems.ems_message_type (Nblade.vscanConnBackPressure), ems.cluster_vendor (NetApp), ems.cluster_model (FAS*, AFF*, ASA*, FDVM*)
- Group By:** ems.cluster_uuid, ems.cluster_vendor, ems.cluster_model, ems.cluster_name, ems.svm_uuid, ems.svm_name

This change brings Metric Monitors and Log Monitors into feature parity by normalizing the “Group By” aspect of Monitor Definitions. This parity will allow customers to clone/duplicate **all** system-defined default Monitors for further customization.

Duplicating

You can now clone (duplicate) the Change Log, Kubernetes Log, and Data Collector Log monitors. This creates a new custom log monitor that you can modify to your specific definitions.

Data Collection (4)					+ Monitor	Bulk Actions	Filter...
<input type="checkbox"/>	Name	Metric / Parameters	Severity	Time Frame	Status		
<input type="checkbox"/>	Acquisition Unit Heartbeat-Critical	logs.cloud_insights.acquisition (source = acquisition_unit", acquisition_unit.status = "Heartbeat Overdue", acquisition_unit.overdue_time = >= 600 sec)	Critical	Once	Active		<div>Duplicate Pause</div>
	Acquisition Unit Heartbeat-Warning	logs.cloud_insights.acquisition (source = acquisition_unit", acquisition_unit.status = "Heartbeat Overdue", acquisition_unit.overdue_time = >= 300 sec)	Warning	Once	Active		

11 New Default ONTAP Monitors covering SnapMirror for Business Continuity

We've added almost a dozen new [system monitors](#) for SnapMirror for Business Continuity (SMBC), which alert on changes to SMBC certificates and ONTAP Mediators.

November 2022

More than 40 new Security, Data Collection, and CVO monitors!

We've added dozens of new system-defined monitors to alert you to potential issues with Cloud Volumes, Security, and Data Protection. Read more about these monitors [here](#).

October 2022

Better and more accurate Ransomware detection with ONTAP Autonomous Ransomware Protection integration

Cloud Secure improves ransomware detection through integration with ONTAP [Autonomous Ransomware Protection](#) (ARP).

Cloud Secure receives ONTAP ARP events on potential volume file encryption activity, and

- Correlates volume encryption events with user activity to identify who is causing the damage,
- Implements automatic response policies to block the attack,
- Identifies which files were affected, helping to recover faster and conduct data breach investigations.

September 2022

Monitors available in Basic Edition

ONTAP [Default monitors](#) now available to use in Cloud Insights Basic Edition. This includes more than 70 infrastructure monitors and 30 workload examples.

ONTAP Power and StorageGRID dashboards

The dashboard gallery includes a new dashboard for ONTAP Power and Temperature as well as four dashboards for StorageGRID. If your environment is collecting ONTAP power metrics and/or StorageGRID data, import these dashboards by selecting **+From Gallery**.

At-a-glance threshold visibility in tables

Conditional Formatting allows you to set and highlight Warning-level and Critical-level thresholds in table widgets, bringing instant visibility to outliers and exceptional data points.

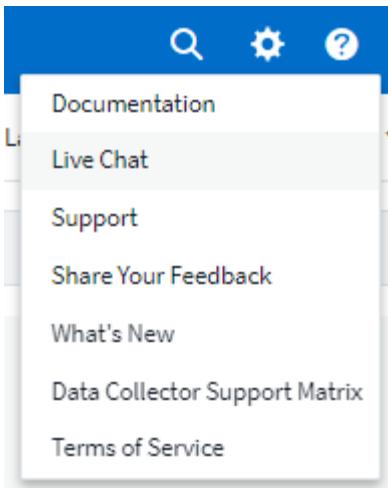
14 items found in 1 group			
Table Row Grouping	Expanded Detail	Metrics & Attributes	
<input type="checkbox"/> All	Storage Pool	capacityRatio.used (%)	<input type="button" value="capacity.provisioned (GiB)"/>
<input type="checkbox"/> All (14)	--	95.15	<input type="button" value="Aggregation"/>
	rtp-sa-cl06-02:aggr_data1_rtp_sa_cl06_02	0.79	<input type="button" value="Unit Display"/>
	rtp-sa-cl06-01:aggr_data1_rtp_sa_cl06_01	2.45	<input type="button" value="Conditional Formatting"/>
	rtp-sa-cl06-02:aggr0_rtp_sa_cl06_02_root	95.15	<input type="button" value="Reset"/>
	rtp-sa-cl06-01:aggr0_rtp_sa_cl06_01_root	95.15	<input type="button" value="Warning"/>
Formatting: <input checked="" type="checkbox"/> Show Expanded Details <input type="button" value="Conditional Formatting"/> <input type="button" value="Background Color + Icon"/> <input type="checkbox"/> Show <input checked="" type="checkbox"/> In Range as green		<input type="checkbox"/> Show <input checked="" type="checkbox"/> In Range as green	<input type="button" value="70 %"/>
		<input type="checkbox"/> Show <input checked="" type="checkbox"/> In Range as green	<input type="button" value="90 %"/>
<input type="button" value="Rename Column"/>			

Security Monitor

Cloud Insights can alert you when it detects that FIPS mode is disabled on the ONTAP system. Read more about [System Monitors](#), and watch this space for more Security Monitors, coming soon!

Chat from Anywhere

Chat with a NetApp Support specialist from any Cloud Insights screen by selecting the new **Help > Live Chat** link. Help is available from the "?" icon in the upper right of the screen.



More visible Insights

If your environment is experiencing an [Insight](#) such as *Shared resources Under Stress* or *Kubernetes Namespaces Running Out of Space*, asset landing pages for resources affected now include links to the Insight itself, providing quicker exploration and troubleshooting.

New Data Collectors

- Amazon S3 (available in Preview)
- Brocade FOS 9.0.x
- Dell/EMC PowerStore 3.0.0.0

Other Data Collector Updates

All data sources are now optimized to resume performance polling after Acquisition Unit updates and/or patches.

Operating System support

The following operating systems are supported with Cloud Insights Acquisition Units, in addition to those [already supported](#):

- Red Hat Enterprise Linux 8.5, 8.6

August 2022

Cloud Insights has a new look!

Starting this month, "Monitor and Optimize" has been renamed **Observability**. You'll find all your favorite features like Dashboards, Queries, Alerts, and Reporting here. In addition, look for Cloud Secure under the new **Security** menu. Note that only the menus have changed; feature functionality remains the same.



Looking for the **Help** menu?

Help now lives in the upper right of the screen.



Not sure where to start? Check out ONTAP Essentials!

ONTAP Essentials is a set of dashboards and workflows that provide detailed views into your NetApp ONTAP inventories, workloads, and data protection, including days-to-full predictions for storage capacity and performance. You can even see if any controllers are running at high utilization. ONTAP Essentials is your ideal place for all of your NetApp ONTAP monitoring needs!

ONTAP Essentials—available in all Editions—is designed to be intuitive to existing ONTAP operators and administrators, easing the transition from ActiveIQ Unified Manager to service-based management tools.



Storage Data families are merged

You asked for it, and now you've got it. Storage base-2 and base-10 data units are now combined into one family, from bits and bytes to tebibits and terabytes, making it easier to display data your way on your dashboards. Data Rates are also now one big family of their own.

iops.total X ▾ Display Unit: iops.total (IO/s)

Dashboard Base Unit iOPS (IO/s) Aggregates

Displayed In Data Storage

bit (b)
kibibit (Kib) kilobit (Kb)
mebibit (Mib)
megabit (Mb)

How much power is my storage using?

Display and monitor your ONTAP storage shelf and node power consumption, temperature, and fan speed, using the netapp_ontap.storage_shelf, netapp_ontap.system_node and netapp_ontap.cluster (power consumption only) metrics.

Cloud Insights (Trial) Tutorial 0% Complete Getting Started ▾ CI Admin ▾

MONITOR & OPTIMIZE ▾ diwlltk / All Metric Queries / Storage Shelf Last 3 Hours Save

netapp_ontap.storage_shelf ▾ Filter By + ? Group by cluster_name x

2 items found in 2 groups

Table Row Grouping	Expanded Detail	Metrics & Attributes								
cluster_name	netapp_ontap.storage_s...	average_...	↑ power	min_ambient...	min_temperat...	max_temperat...	average_temp...	average_fan_s...	min_fan_spe...	
rtp-sa-cl06 (1)	1.0	23.00	0.26	23.00	25.00	38.00	30.86	2,997.50	2,970.00	
umeng-aff300-01-02 (1)	1.1	27.00	0.15	27.00	30.00	41.00	32.40	2,970.00	2,940.00	

Share your feedback! We want your input to help

Features graduated from Preview

The following features have moved out of Preview and are now available to all customers:

Feature	Description
Kubernetes Namespaces Running out of Space	<p>The <i>Kubernetes Namespaces Running Out of Space</i> Insight gives you a view into workloads on your Kubernetes namespaces that are at risk of running out of space, with an estimate for the number of days remaining before each space becomes full.</p> <p>Read More</p>
Shared Resource Under Stress	<p>The <i>Shared Resource Under Stress</i> insight uses AI/ML to automatically identify where resource contention is causing performance degradation in your environment, highlights any workloads impacted by it, and provides recommended actions to remediate, letting you solve performance issues more quickly.</p> <p>Read More</p>
Cloud Secure – Block user access on attack	<p>Greater protection for your business-critical data with the ability to block user access when an attack is detected.</p> <p>Access can be blocked automatically, using Automated Response Policies, or manually from the alert or user details pages.</p> <p>Read More</p>

How's my data collection health?

Cloud Insights provides two new heartbeat monitors for your Acquisition Units, as well as two monitors to alert you to data collector failures. These can be used to alert you quickly to data collection issues.

The following monitors are now available in the *Data Collection* monitor group:

- Acquisition Unit Heartbeat-Critical
- Acquisition Unit Heartbeat-Warning
- Collector Failed
- Collector Warning

Note that these monitors are in *Paused* state by default. Activate them to be alerted about data collection issues.

Auto-Renewing API Tokens

API Access Tokens can now be set for auto-renewal. By enabling this feature, new/refreshed API Access Tokens will automatically be generated for expiring tokens. Cloud Insights agents using an expiring token will automatically be updated to use the corresponding new/refreshed API Access Token, allowing them to continue to operate seamlessly. Simply check the “Renew token automatically” box when creating your token. This feature is currently supported on Cloud Insights agents running on the Kubernetes platform with the latest NetApp Kubernetes Monitoring Operator.

Basic Edition gives you more than before

Your trial is ending but you're not yet sure whether a subscription is right for you? Basic Edition has always given you a chance to continue using Cloud Insights with your current ONTAP data collector, but now you can continue capturing VMWare version, topology, and IOPS/Throughput/Latency data as well. NetApp customers with premium support on their storage systems will also be entitled to support for Cloud Insights.

Ready to learn more?

Check out the **Learning Center** section of the Help > Support page for links to NetApp University Cloud Insights course offerings!

Operating System support

The following operating system is supported with Cloud Insights Acquisition Units, in addition to those [already supported](#):

- Windows 11

June 2022

Kubernetes cluster saturation and other details

Cloud Insights makes it easier than ever to explore your Kubernetes environment, with an improved cluster detail page that provides Saturation details as well as a cleaner view into Namespaces and Workloads.



The Cluster list page also gives you a quick view of saturation, in addition to Node, Pod, Namespace, and Workload counts:

Filter By + ?

Clusters (2)

Name ↑	Overall Saturation (%)	CPU Saturation (%)	Memory Saturation (%)	Storage Saturation (%)	Nodes	Pods	Namespaces	Workloads
self	56	25	56	31	2	63	18	68
setoK3s	4	2	3	4	2	9	5	7

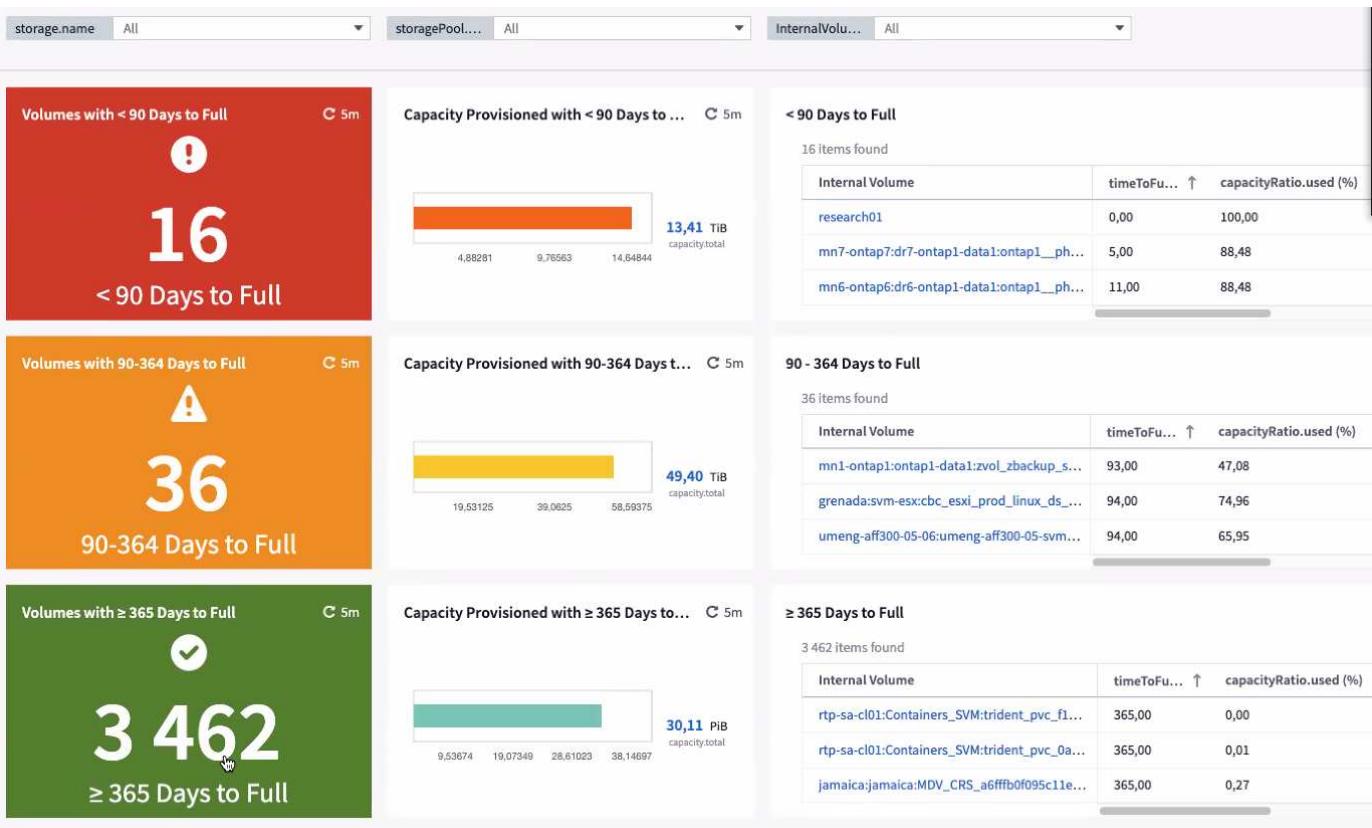
How old is your Kubernetes cluster?

Is your cluster just starting in the world, or has it experienced a long digital life? Age has been added as a time metric collected for Kubernetes Nodes.

2 items found in 2 groups			
Table Row Grouping		Expanded Detail	Metrics & Attributes
node_name ↑	kubernetes_cluster	kubernetes.node	age (day)
ci-aumonitor-1 (1)	aumonitor	ci-aumonitor-1	10.82
ci-aumonitor-2 (1)	aumonitor	ci-aumonitor-2	10.82

Capacity Time-to-Full forecasting

Cloud Insights provides a dashboard to forecast the number of days until capacity runs out for each Internal Volume monitored. These values can help to significantly reduce the risk of an outage.



TTF counters are also available for Storage, Storage Pool, and Volume. Keep watching this space for additional dashboards for these objects.

Note that Time-to-Full forecasting is moving out of *Preview* and will be rolled out to all customers.

What's changed in my environment?

ONTAP change log entries can be viewed in the log explorer.



Operating System support

The following operating systems are supported with Cloud Insights Acquisition Units, in addition to those [already supported](#):

- CentOS Stream 9
- Windows 2022

Updated Telegraf Agent

The agent for ingestion of telegraf integration data has been updated to version **1.22.3**, with performance and security improvements.

Users wishing to update can refer to the appropriate upgrade section of the [Agent Installation](#) documentation. Previous versions of the agent will continue to function with no user action required.

Preview Features

Cloud Insights regularly highlights a number of exciting new preview features. If you are interested in previewing one or more of these features, contact your [NetApp Sales Team](#) for more information.

Feature	Description
Kubernetes Namespaces Running out of Space	<p>The <i>Kubernetes Namespaces Running Out of Space</i> Insight gives you a view into workloads on your Kubernetes namespaces that are at risk of running out of space, with an estimate for the number of days remaining before each space becomes full.</p> <p>Read More</p>
Cloud Secure – block user access on attack	<p>Greater protection for your business-critical data with the ability to block user access when an attack is detected.</p> <p>Access can be blocked automatically, using Automated Response Policies or manually from the alert or user details pages.</p> <p>Read More</p>
Shared Resource Under Stress	<p>The <i>Shared Resource Under Stress</i> insight uses AI/ML to automatically identify where resource contention is causing performance degradation in your environment, highlights any workloads impacted by it, and provides recommended actions to remediate, letting you solve performance issues more quickly.</p> <p>Read More</p>

May 2022

Chat live with NetApp Support

You can now chat live with NetApp Support personnel! On the Help > Support page, simply click the Chat icon or click *Chat* in the "Contact Us" section to start a chat session. Chat support is available US weekdays for Standard and Premium Edition users.



Kubernetes Operator

We've made it easier to get you up and running with Cloud Insights' advanced Kubernetes monitoring and cluster explorer.

The [NetApp Kubernetes Monitoring Operator](#) (NKMO) is the preferred method for installing Kubernetes for Cloud Insights Insights, for more flexible configuration of monitoring in fewer steps, as well as enhanced opportunities for monitoring other software running in the K8s cluster.

Click the link above for more information and pre-requisites

Manage Users and Invites with API

You can now manage users and invites using Cloud Insights' powerful API. Read more in the [API Swagger Documentation](#).

Data Collection Alerts

Don't miss out on critical metrics due to a failed collector!

It's easier than ever to keep track of your data collectors with new [alerts](#) for data collector and acquisition unit failures.

Note that these Monitors are *Paused* by default. To enable, navigate to your monitors page and locate and resume "Acquisition Unit Shutdown" and "Collector Failed"

Alert on ONTAP storage changes

Don't let unexpected storage changes lead to outages!

You can now configure Cloud Insights to alert when modification or removal of FlexVols, nodes and SVMs are detected on ONTAP systems.

Preview Features

Cloud Insights regularly highlights a number of exciting new preview features. If you are interested in previewing one or more of these features, contact your [NetApp Sales Team](#) for more information.

Feature	Description
Kubernetes Namespaces Running out of Space	The <i>Kubernetes Namespaces Running Out of Space</i> Insight gives you a view into workloads on your Kubernetes namespaces that are at risk of running out of space, with an estimate for the number of days remaining before each space becomes full. Read More
Internal Volume and Volume Capacity Time-to-Full forecasting	Cloud Insights is able to prognose the number of days until capacity runs out for each Internal Volume and Volume monitored. This value can help to significantly reduce the risk of an outage.
Cloud Secure – block user access on attack	Greater protection for your business-critical data with the ability to block user access when an attack is detected. Access can be blocked automatically, using Automated Response Policies or manually from the alert or user details pages. Read More
Shared Resource Under Stress	The <i>Shared Resource Under Stress</i> insight uses AI/ML to automatically identify where resource contention is causing performance degradation in your environment, highlights any workloads impacted by it, and provides recommended actions to remediate, letting you solve performance issues more quickly. Read More

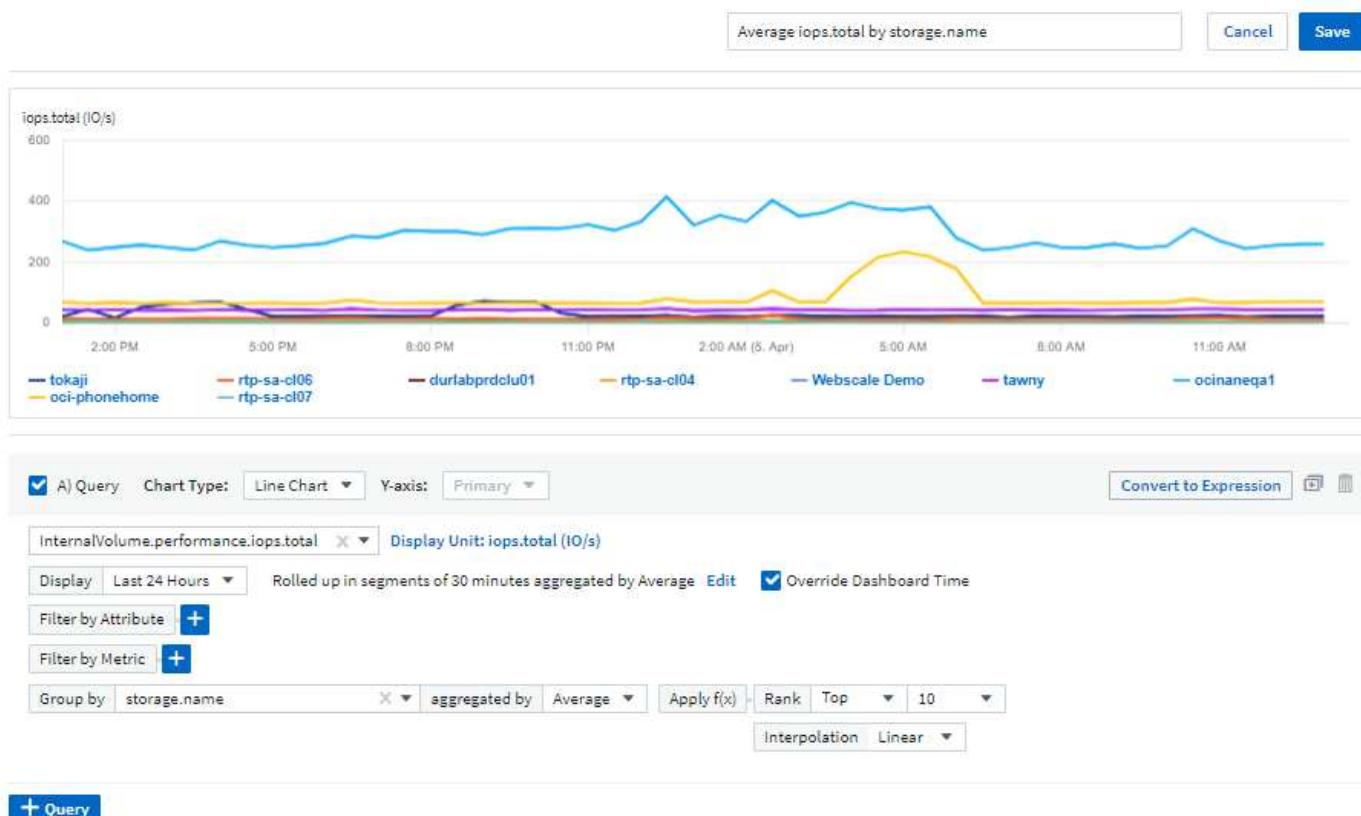
April 2022

Share your Feedback!

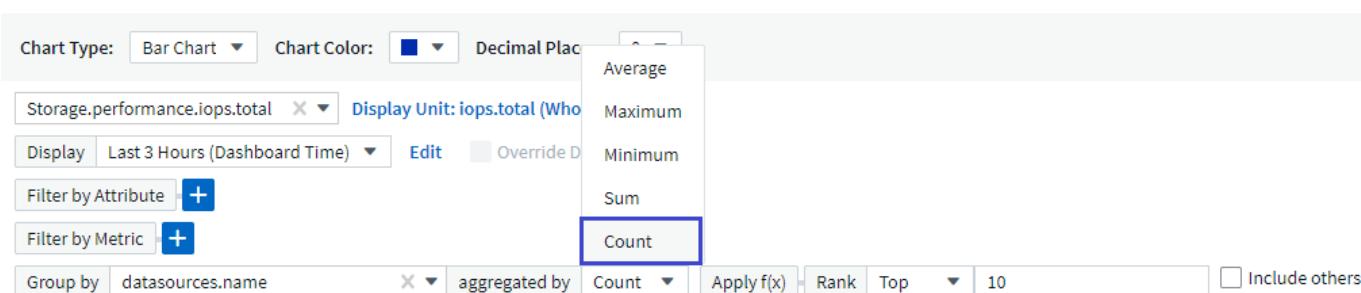
We want your input to help shape Cloud Insights. Earn points and prizes by participating in NetApp's **Insights to Action** program. [Sign up now!](#)

Updated Dashboard Editor

We've overhauled our dashboard creation tools to make it easier for you to visualize your data even more quickly. Navigate to the "Dashboards" page of Cloud Insights to edit an existing dashboard, add one from our dashboard gallery, or create a new dashboard of your own to check it out.



A new Count aggregation method has also been introduced. When grouping data in bar chart, column chart, and pie chart widgets, you can quickly and easily show the number of relevant objects for the selected metric.



Additionally, line charts now allow you to select one of three [interpolation](#) methods:

- None - No interpolation is done
- Linear - Interpolates a data point between the existing points
- Stair - Uses the previous data point as the interpolated data point

Enhanced Monitoring for Your Kubernetes Infrastructure

Cloud Insights keeps you on top of changes in your Kubernetes environment by alerting you when pods, daemonsets, and replicaset are created or removed, as well as when new deployments are created. Kubernetes monitors default to *paused* state, so you should enable only the specific ones you need.

Preview Features

Cloud Insights regularly highlights a number of exciting new preview features. If you are interested in previewing one or more of these features, contact your [NetApp Sales Team](#) for more information.

Feature	Description
Internal Volume and Volume Capacity Time-to-Full forecasting	Cloud Insights is able to prognose the number of days until capacity runs out for each Internal Volume and Volume monitored. This value can help to significantly reduce the risk of an outage.
Cloud Secure – block user access on attack	Greater protection for your business-critical data with the ability to block user access when an attack is detected. Access can be blocked automatically, using Automated Response Policies or manually from the alert or user details pages. Read More
Shared Resource Under Stress	The Shared Resource Under Stress insight uses AI/ML to automatically identify where resource contention is causing performance degradation in your environment, highlights any workloads impacted by it, and provides recommended actions to remediate, letting you solve performance issues more quickly. Read More

New Data Collector

- **Cohesity SmartFiles** - This REST API-based collector will acquire a Cohesity cluster, discovering the “Views” (as CI Internal Volumes), the various nodes, as well as collecting performance metrics.

Other Data Collector Updates

Collection and display of performance data has been improved on the following data collectors:

- Brocade CLI
- Dell/EMC VPLEX, PowerStore, Isilon/PowerScale, VNX Block/Clariion CLI, XtremIO, Unity/VNXe
- Pure FlashArray

These performance enhancements are already available in all NetApp data collectors as well as VMware and

Cisco, and will be rolled out to all other data collectors over the next few months.

March 2022

Cloud Connection for ONTAP 9.9+

The [NetApp Cloud Connection for ONTAP 9.9+](#) data collector eliminates the need to install an external acquisition unit, thereby simplifying troubleshooting, maintenance, and initial deployment.

New FSx for NetApp ONTAP Monitors

Monitoring your FSx for NetApp ONTAP environment is easy with new [system-defined monitors](#) for both infrastructure (metrics) and workloads (logs).

FSX Infrastructure (1)					
<input type="checkbox"/>	Name	Metric / Parameters	Severity	Time Frame	Status
	FSx Volume Cache Miss Ratio	netapp_ontap.workload_volume.cache_miss_ratio	⚠ Warning @ > 95 % ❗ Critical @ > 100 %	For 30 minutes	() Paused
FSX Workload Examples (5)					
<input type="checkbox"/>	Name	Metric / Parameters	Severity	Time Frame	Status
	FSx Snapshot Reserve Space is Full	netapp_ontap.workload_volume.snapshot_size_used_percent	⚠ Warning @ > 90 % ❗ Critical @ > 95 %	Once	() Paused
	FSx Volume Capacity is Full	netapp_ontap.workload_volume.size_used_percent	⚠ Warning @ > 85 % ❗ Critical @ > 95 %	Once	() Paused
	FSx Volume High Latency	netapp_ontap.workload_volume.total_latency	⚠ Warning @ > 1,000 µs ❗ Critical @ > 2,000 µs	For 5 minutes	() Paused
	FSx Volume Inodes Limit	netapp_ontap.workload_volume.inodes_used_percent	⚠ Warning @ > 85 % ❗ Critical @ > 95 %	Once	() Paused
	FSx Volume Qtree Quota Overcommit	netapp_ontap.workload_volume.qtree_quota_commit_percent	⚠ Warning @ > 95 % ❗ Critical @ > 100 %	Once	() Paused

New Cloud Secure features available to all

Your environment is more secure than ever with the following Cloud Secure features now generally available:

Feature	Description
Data Destruction – File Deletion attack detection	Detect abnormal large-scale file deletion activity, block malicious file access by malicious users, and take automatic snapshots with automatic response policies.
Separate notifications for Warnings and Alerts	Warning and Alert notifications can be sent to separate recipients, ensuring the right team can stay informed

Updated Telegraf Agent

The agent for ingestion of telegraf integration data has been updated to version **1.21.2**, with performance and security improvements.

Users wishing to update can refer to the appropriate upgrade section of the [Agent Installation](#) documentation. Previous versions of the agent will continue to function with no user action required.

Data Collector Updates

- The Broadcom Fibre Channel Switches data collector has been optimized to reduce the number of CLI commands issued with each inventory poll.
-

February 2022

Cloud Insights addresses Apache Log4j vulnerabilities

Customer security is a top priority at NetApp. Cloud Insights includes updates to its software libraries to address the recent Apache Log4j vulnerabilities.

Please refer to the following on NetApp's Product Security Advisory website:

[CVE-2021-44228](#)

[CVE-2021-45046](#)

[CVE-2021-45105](#)

You can read more about these vulnerabilities and NetApp's response at the [NetApp Newsroom](#).

Kubernetes Namespace Detail Page

Exploring your Kubernetes environment is now better than ever, with informative detail pages for your cluster's namespaces. The namespace detail page provides a summary of all the assets used by a namespace, including all the backend storage resources and their capacity utilizations.



December 2021

Deeper integration for ONTAP systems

Simplify alerting for ONTAP hardware failures and more with new integration with NetApp Event Management System (EMS).

[Explore and alert](#) on low-level ONTAP messages in Cloud Insights to inform and improve troubleshooting workflows and further reduce reliance on ONTAP element management tooling.

Querying Logs

For ONTAP systems, Cloud Insights Queries include a powerful [Log Explorer](#), allowing you to easily investigate and troubleshoot EMS log entries.

The screenshot shows the Cloud Insights interface with the 'QUERIES' tab selected. On the left, there's a sidebar with a magnifying glass icon. The main area has two sections: 'Metric Queries' (763 entries) and 'Log Queries' (3 entries, marked as 'NEW'). Each section has a 'New' button.

Data Collector-level notifications.

In addition to system-defined and custom-created Monitors for alerting, you can also set alert notifications for ONTAP data collectors, allowing you to specify recipients for collector-level alerts, independent of other monitor alerts.

Greater flexibility of Cloud Secure roles

Users can be granted access to Cloud Secure features based on [roles](#) set by an administrator:

Role	Cloud Secure Access
Administrator	Can perform all Cloud Secure functions, including those for Alerts, Forensics, data collectors, automated response policies, and APIs for Cloud Secure. An Administrator can also invite other users but can only assign Cloud Secure roles.
User	Can view and manage Alerts and view Forensics. User role can change alert status, add a note, take snapshots manually, and block user access.
Guest	Can view Alerts and Forensics. Guest role cannot change alert status, add a note, take snapshots manually, or block user access.

Operating System support

CentOS 8.x support is being replaced with [CentOS 8 Stream](#) support. CentOS 8.x will reach End-of-Life on December 31, 2021.

Data Collector Updates

A number of Cloud Insights data collector names have been added to reflect vendor changes:

Vendor/Model	Previous Name
Dell EMC PowerScale	Isilon
HPE Alletra 9000 / Primera	3PAR
HPE Alletra 6000	Nimble

November 2021

Adaptive Dashboards

New variables for attributes and the ability to use variables in widgets.

Dashboards are now more powerful and flexible than ever. Build adaptive dashboards with attribute variables to quickly filter dashboards on the fly. Using these and other pre-existing [variables](#) you can now create one high level dashboard to see metrics for your entire environment, and seamlessly filter down by resource name, type, location, and more. Use number variables in widgets to associate raw metrics with costs, for example cost per GB for storage as a service.

The screenshot shows the Cloud Insights dashboard configuration interface. On the left, a sidebar titled 'Variables' lists categories: Attribute, Annotation, Text, Number, Boolean, and Date. An 'Attribute' variable is currently selected. A modal dialog box is open, titled 'Attribute', with a search input field containing 'ontap name'. Below the input field is a dropdown menu showing 'Objects containing "aggr_name"'. A list of matching attribute names is displayed, all of which include the prefix 'netapp_ontap.' followed by the attribute name: aggregate.aggr_name, aggregate.cluster_name, aggregate.node_name, aggregate.owner_name, cifs_node.cluster_name, cifs_node.node_name, cifs_vserver.cluster_name, and cluster.cluster_name.

Access the Reporting Database via API

Enhanced capabilities for integration with third party reporting, ITSM, and automation tools: Cloud Insights' powerful [API](#) allows users to query the Cloud Insights Reporting database directly, without going through the

Cognos Reporting environment.

Pod tables on VM Landing Page

Seamless navigation between VMs and the Kubernetes Pods using them: for improved troubleshooting and performance headroom management, a table of associated Kubernetes Pods will now appear on VM landing pages.

Kubernetes Pods				
15 items found				
pod_name ↑	kubernetes_cluster	namespace	owner_kind	owner_name
calico-kube-controllers-649b7b795b-ktp2n	ci-rancher	kube-system	ReplicaSet	calico-kube-controllers-649b7b795b
canal-mpvhx	ci-rancher	kube-system	DaemonSet	canal
cattle-cluster-agent-74c7797cc5-b9jhz	ci-rancher	cattle-system	ReplicaSet	cattle-cluster-agent-74c7797cc5
cattle-node-agent-bn225	ci-rancher	cattle-system	DaemonSet	cattle-node-agent
coredns-autoscaler-79599b9dc6-dtwpj	ci-rancher	kube-system	ReplicaSet	coredns-autoscaler-79599b9dc6

Data Collector Updates

- ECS now reports firmware for storage and node
- Isilon has improved prompt detection
- Azure NetApp Files collects performance data more quickly
- StorageGRID now supports Single Sign-On (SSO)
- Brocade CLI properly reports model for X&-4

Additional Operating Systems supported

The Cloud Insights Acquisition Unit supports the following operating systems, in addition to those already supported:

- Centos (64-bit) 8.4
- Oracle Enterprise Linux (64-bit) 8.4
- Red Hat Enterprise Linux (64-bit) 8.4

October 2021

Filters on K8S Explorer pages

[Kubernetes Explorer](#) page filters give you focused control of the data displayed for your Kubernetes cluster, node, and pod exploration.

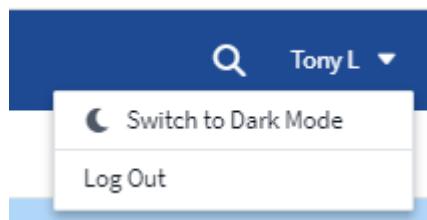
K8s Data for Reporting

Kubernetes data is now available for use in Reporting, allowing you to create chargeback or other reports. In order for Kubernetes chargeback data to be passed to Reporting, you must have an active connection to, and Cloud Insights must be receiving data from, your Kubernetes cluster as well as its back-end storage. If there is no data received from the back-end storage, Cloud Insights can not send Kubernetes object data to Reporting.



Dark Theme has arrived

Many of you asked for a dark theme, and Cloud Insights has answered. To switch between light and dark theme, click the drop-down next to your user name.





Data Collector Support

We've made some improvements in Cloud Insights Data Collectors. Here are some highlights:

- New collector for Amazon FSx for ONTAP

September 2021

Performance Policies are now Monitors

Monitors and Alerts have supplanted Performance Policies and Violations throughout Cloud Insights. [Alerting with Monitors](#) provides greater flexibility and insight into potential problems or trends in your environment.

Autocomplete Suggestions, Wildcards, and Expressions in Monitors

When creating a monitor for alerting, typing in a filter is now predictive, allowing you to easily search for and find the metrics or attributes for your monitor. Additionally, you are given the option to create a wildcard filter based on the text you type.

1 Select a metric to monitor

The screenshot shows a search bar at the top with the text "StoragePool.performance.utilization.read". Below it is a filter interface. The "name" field has "sas1" entered. A dropdown menu is open, showing suggestions: "Create wildcard containing 'sas1'", "tawny03:tawny03sas1", "tawny04:tawny04sas1", and "None". There are also "Group" and "Avg" buttons.

Updated Telegraf Agent

The agent for ingestion of telegraf integration data has been updated to version **1.19.3**, with performance and security improvements.

Users wishing to update can refer to the appropriate upgrade section of the [Agent Installation](#) documentation. Previous versions of the agent will continue to function with no user action required.

Data Collector Support

We've made some improvements in Cloud Insights Data Collectors. Here are some highlights:

- Microsoft Hyper-V collector now uses PowerShell instead of WMI
- Azure VMs and VHD collector is now up to 10 times faster due to parallel calls
- HPE Nimble now supports federated and iSCSI configurations

And since we're always improving Data Collection, here are some other recent changes of note:

- New collector for EMC Powerstore
- New collector for Hitachi Ops Center
- New collector for Hitachi Content Platform
- Enhanced ONTAP collector to report Fabric Pools
- Enhanced ANF with Storage Pool and Volume performance
- Enhanced EMC ECS with Storage Nodes and Storage performance as well as the Object Count in buckets
- Enhanced EMC Isilon with Storage Node and Qtree metrics
- Enhanced EMC Symetrix with volume QOS limit metrics
- Enhanced IBM SVC and EMC PowerStore with Storage Nodes parent serial number

August 2021

New Audit Page User Interface

The [Audit page](#) provides a cleaner interface and now allows the export of audit events to .CSV file.

Enhanced User Role Management

Cloud Insights now allows even greater freedom for assigning user roles and access controls. Users can now be assigned granular permissions for monitoring, reporting, and Cloud Secure separately.

This means you can allow more users administrative access to monitoring, optimization, and reporting functions whilst restricting access to your sensitive Cloud Secure audit and activity data to only those that need it.

[Find out more](#) about the different levels of access in the Cloud Insights documentation.

June 2021

Autocomplete Suggestions, Wildcards, and Expressions in Filters

With this release of Cloud Insights, you no longer need to know all the possible names and values on which to filter in a query or widget. When filtering, you can simply start typing and Cloud Insights will suggest values based on your text. No more looking up Application names or Kubernetes attributes ahead of time just to find the ones you want to show in your widget.

As you type in a filter, the filter displays a smart list of results from which you can choose, as well as the option to create a **wildcard filter** based on the current text. Selecting this option will return all results that match the wildcard expression. You can of course also select multiple individual values that you want added to the filter.

The screenshot shows a filtering interface. At the top, there is a search bar containing "kubernetes.pod". Below it, a "Filter By" section has "pod_name" selected. A dropdown menu is open over the input field, showing the value "ingest". To the right of the dropdown are buttons for "X", "+", and "?". Below the dropdown, a tooltip says "Create wildcard containing \"ingest\"". The dropdown menu lists three items: "ci-service-datalake-ingestion-85b5bdfd6d-2qbwr", "service-foundation-ingest-767dfd5bfc-vxd5p", and "None". At the bottom left, it says "71 items found" and "Table Row Grouping".

Additionally, you can create **expressions** in a filter using NOT or OR, or you can select the "None" option to filter for null values in the field.

Read more about [filtering options](#) in queries and widgets.

APIs available by Edition

Cloud Insights' powerful APIs are more accessible than ever, with Alerts APIs now available in Standard and Premium Editions.

The following APIs are available for each Edition:

API Category	Basic	Standard	Premium
Acquisition Unit	✓	✓	✓
Data Collection	✓	✓	✓
Alerts		✓	✓
Assets		✓	✓
Data Ingestion		✓	✓

Kubernetes PV and Pod Visibility

Cloud Insights provides visibility into the back-end storage for your Kubernetes environments, giving you insight to your Kubernetes Pods and Persistent Volumes (PVs). You can now track PV counters such as IOPS, latency, and throughput from a single Pod's usage through a PV counter to a PV and all the way to the back-end storage device.

On a Volume or Internal Volume landing page, two new tables are displayed:

Kubernetes PVs
C 5m

2 items found

PV ↑	Cluster	PV Capacity (GiB)	Phase	StorageClass
cvo-shared-storage-pv	QA_K8S_CLUSTER	0.73	Bound	
test-mysql-shared-storage-pv	QA_K8S_CLUSTER	7.32	Bound	

Kubernetes Pods
C 5m

2 items found

Pod ↑	Cluster	Namespace	PV	Workload Type	Workload	Latency - Total ...	IOPS - T
cvo-mypod-pvc	QA_K8S_CLU...	k8testns	cvo-shared-storage			0.00	
test-mysql-0	QA_K8S_CLU...	k8testns	test-mysql-shared-	StatefulSet	test-mysql	0.19	2.72

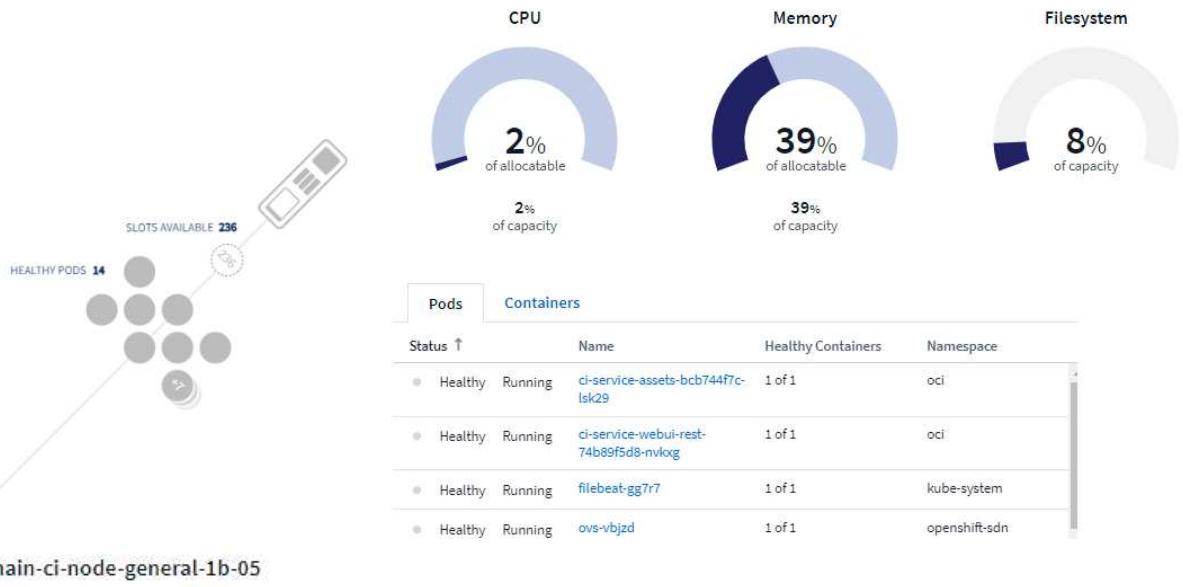
Note that to take advantage of these new tables, it is recommended to uninstall your current Kubernetes agent, and install it fresh. You must also install Kube-State-Metrics version 2.1.0 or later.

Kubernetes Node to VM links

On a Kubernetes Node page, you can now click to open the Node's VM page. The VM page also includes a link back to the Node itself.

14
Pods **14** Healthy **0** Alerting

Labels - Node IP 10.30.27.178 Virtual Machine main-ci-node-general-1b-05 



NetApp /  main-ci-node-general-1b-05

Virtual Machine Summary				 5m
Power State: On	Latency - Total: 1.21 ms	Hypervisor IP: US-EAST-1B		
Guest State: Running	IOPS - Total: 11.06 IO/s	Hypervisor OS: Amazon AWS EC2		
Datastore: i-01b052b8d843994e7	Throughput - Total: 0.06 MB/s	Hypervisor FC Fabrics: 0		
CPU Utilization - Total: 3.89 %	DNS Name: ip-10-178.ec2.internal	Hypervisor CPU Utilization: N/A		
Memory Utilization - Total: N/A	IP:	Hypervisor Memory Utilization: N/A		
Memory: 32.0 GB	OS: CentOS Linux 7 x86_64 HVM EBS ENA 1901_01-	Kubernetes Node: ip-10-30-27-178.ec2.internal		
Capacity - Total: 200.0 GB	Processors: 8	Alert Monitors:		
Capacity - Used: N/A	Hypervisor Name: us-east-1b	VM Capacity		
		VM IOPS		
		View Topology		

Alert Monitors replacing Performance Policies

To enable the added benefits of multiple thresholds, webhook and email alert delivery, alerting on all metrics using a single interface, and more, Cloud Insights will be converting Standard and Premium Edition customers from **Performance Policies** to **Monitors** during the months of July and August, 2021. Learn more about [Alerts and Monitors](#), and stay tuned for this exciting change.

Cloud Secure supports NFS

Cloud Secure now supports NFS for ONTAP data collection. Monitor SMB and NFS user access to protect your data from ransomware attacks.

Additionally, Cloud Secure supports Active-Directory and LDAP user directories for collection of NFS user attributes.

Cloud Secure snapshot purge

Cloud Secure automatically deletes snapshots based on the Snapshot Purge Settings, to save storage space and reduce the need for manual snapshot deletion.

Snapshot Purge Settings X

Define purge periods to automatically delete snapshots taken by Cloud Secure.

Attack Automated Response

Delete Snapshot after

Warning Automated Response

Delete Snapshot after

User Created

Delete Snapshot after

Cloud Secure data collection speed

A single data collector agent system can now post up to 20,000 events per second to Cloud Secure.

May 2021

Here are some of the changes we've made in April:

Updated Telegraf Agent

The agent for ingestion of telegraf integration data has been updated to version 1.17.3, with performance and security improvements.

Users wishing to update can refer to the appropriate upgrade section of the [Agent Installation](#) documentation.

Previous versions of the agent will continue to function with no user action required.

Add Corrective Actions to an Alert

You can now add an optional description as well as additional insights and/or corrective actions when creating or modifying a Monitor by filling in the **Add an Alert Description** section. The description will be sent with the alert. The *insights and corrective actions* field can provide detailed steps and guidance for dealing with alerts and will be displayed in the summary section of the alert landing page.

4 Add an alert description (optional)

Add a description
Enter a description that will be sent with this alert (1024 character limit)

Add insights and corrective actions
Enter a url or details about the suggested actions to fix the issue raised by the alert

Cloud Insights APIs for All Editions

API access is now available in all editions of Cloud Insights.

Users of Basic edition can now automate actions for Acquisition Units and Data Collectors, and Standard Edition users can query metrics and ingest custom metrics.

Premium edition continues to allow full use of all API categories.

API Category	Basic	Standard	Premium
Acquisition Unit	✓	✓	✓
Data Collection	✓	✓	✓
Assets		✓	✓
Data Ingestion		✓	✓
Data Warehouse			✓

For details on API usage, please refer to the [API documentation](#).

April 2021

Easier Management of Monitors

[Monitor Grouping](#) simplifies the management of monitors in your environment. Multiple monitors can now be grouped together and paused as one. For example, if you have an update occurring on a stack of infrastructure, you can pause alerts from all those devices via one click.

Monitor groups is the first part of an exciting new feature bringing improved management of ONTAP devices to Cloud Insights.

The screenshot shows a list of monitor groups. At the top, there is a header 'Monitor Groups (5)' with a search bar below it. Below the search bar is a list of categories: 'All Monitors (5)', 'Custom Monitors (5)', 'Agent Monitors (3)', and 'ONTAP Aggregate Monitors (2)'. Each category has a three-dot menu icon to its right.

Enhanced Alerting Options Using Webhooks

Many commercial applications support [Webhooks](#) as a standard input interface. Cloud Insights now supports many of these delivery channels, providing default templates for Slack, PagerDuty, Teams, and Discord, in addition to providing customizable generic webhooks to support many other applications.

3 Set up team notification(s) (alert your team via email, or Webhook)

The screenshot shows two sections for setting up team notifications. Each section has a 'By Webhook' label, a 'Notify team on' dropdown, and a 'Use Webhook(s)' dropdown. The first section's 'Notify team on' dropdown is set to 'Critical, Warning' and its 'Use Webhook(s)' dropdown contains 'PagerDuty Trigger'. The second section's 'Notify team on' dropdown is set to 'Resolved' and its 'Use Webhook(s)' dropdown contains 'PagerDuty Resolve'.

Improved Device Identification

To improve monitoring and troubleshooting as well as deliver accurate reporting, it is helpful to understand the names of devices rather than their IP addresses or other identifiers. Cloud Insights now incorporates an automatic way to identify the names of storage and physical host devices in the environment, using a rule-based approach called [Device Resolution](#), available in the **Manage** menu.

You asked for more!

A popular ask by customers has been for more default options for visualizing the range of data, so we have added the following five new choices that are now available throughout the service via the time range picker:

- Last 30 Minutes
- Last 2 Hours
- Last 6 Hours
- Last 12 Hours
- Last 2 Days

Multiple Subscriptions in one Cloud Insights Environment

Starting April 2, Cloud Insights supports multiple subscriptions of the same edition type for a customer in a single Cloud Insights instance. This enables customers to co-term parts of their Cloud Insights subscription with infrastructure purchases. Contact NetApp Sales for assistance with multiple subscriptions.

Choose Your Path

While setting up Cloud Insights, you can now choose whether to start with Monitoring and Alerting or Ransomware and Insider Threat Detection. Cloud Insights will configure your starting environment based on the path you choose. You can configure the other path at any time afterward.

Easier Cloud Secure Onboarding

And it is easier than ever to start using Cloud Secure, with a new step-by-step setup checklist.



Secure Your Data from Ransomware & Insider Threat

- Ransomware & insider threat detection
- User data access auditing

Setting up Cloud Secure

- ✓ Add an [Agent](#) on server or VM to collect data ([system requirements](#)).
- ✓ Configure a [User Directory Collector](#) to collect user attributes from active directories (optional step).
- ✓ Configure a [Data Collector](#) to collect file access activity on your storage devices.
- ✓ Define [Automated Response Policies](#) to take automatic action in the event of an attack.

User activity data will appear in the [Forensics](#) section

As always, we love to hear your suggestions! Send them to ng-cloudinsights-customerfeedback@netapp.com.

February 2021

Updated Telegraf Agent

The agent for ingestion of telegraf integration data has been updated to version 1.17.0, which includes vulnerability and bug fixes.

Cloud Cost Analyzer

Experience the power of Spot by NetApp with Cloud Cost, which provides a detailed [cost analysis](#) of past, present, and estimated spending, providing visibility into cloud usage in your environment. The Cloud Cost dashboard delivers a clear view of cloud expenses and a drill down into individual workloads, accounts, and services.

Cloud Cost can help with these major challenges:

- Tracking and monitoring your cloud expenses
- Identifying waste and potential optimization areas
- Delivering executable action items

Cloud Cost is focused on monitoring. Upgrade to the full Spot by NetApp account to enable automatic cost

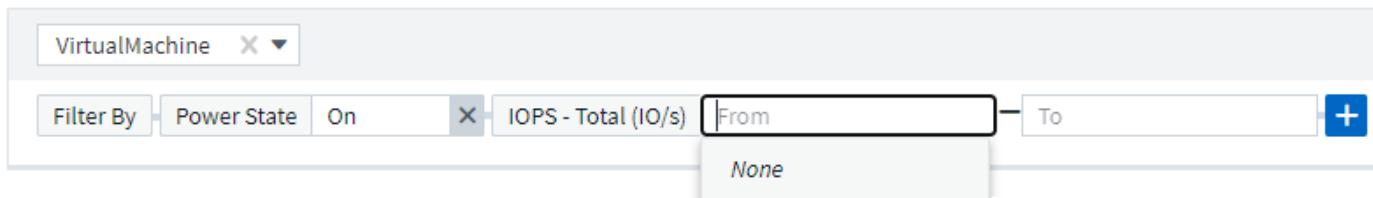
saving and environment optimization.

Querying for objects having null values using filters

Cloud Insights now allows searching for attributes and metrics having null/none values through the use of filters. You can perform this filtering on any attributes/metrics in the following places:

- On the Query page
- In Dashboard widgets and page variables
- On the Alerts list page
- When creating Monitors

To filter for null/none values, simply select the *None* option when it appears in the appropriate filter drop-down.



Multi-Region Support

Starting today we offer the Cloud Insights service in different regions across the globe, which facilitates performance and increases security for customers based outside the United States. Cloud Insights/Cloud Secure stores information according to the region in which your environment is created.

Click [here](#) for more information.

January 2021

Additional ONTAP Metrics Renamed

As part of our continuing effort to improve efficiency of data-gathering from ONTAP systems, the following ONTAP metrics have been renamed.

If you have existing dashboard widgets or queries using any of these metrics, you will need to edit or re-create them to use the new metric names.

Previous Metric Name	New Metric Name
netapp_ontap.disk_constituent.total_transfers	netapp_ontap.disk_constituent.total_iops
netapp_ontap.disk.total_transfers	netapp_ontap.disk.total_iops
netapp_ontap.fcp_lif.read_data	netapp_ontap.fcp_lif.read_throughput
netapp_ontap.fcp_lif.write_data	netapp_ontap.fcp_lif.write_throughput
netapp_ontap.iscsi_lif.read_data	netapp_ontap.iscsi_lif.read_throughput
netapp_ontap.iscsi_lif.write_data	netapp_ontap.iscsi_lif.write_throughput

Previous Metric Name	New Metric Name
netapp_ontap.lif.recv_data	netapp_ontap.lif.recv_throughput
netapp_ontap.lif.sent_data	netapp_ontap.lif.sent_throughput
netapp_ontap.lun.read_data	netapp_ontap.lun.read_throughput
netapp_ontap.lun.write_data	netapp_ontap.lun.write_throughput
netapp_ontap.nic_common.rx_bytes	netapp_ontap.nic_common.rx_throughput
netapp_ontap.nic_common.tx_bytes	netapp_ontap.nic_common.tx_throughput
netapp_ontap.path.read_data	netapp_ontap.path.read_throughput
netapp_ontap.path.write_data	netapp_ontap.path.write_throughput
netapp_ontap.path.total_data	netapp_ontap.path.total_throughput
netapp_ontap.policy_group.read_data	netapp_ontap.policy_group.read_throughput
netapp_ontap.policy_group.write_data	netapp_ontap.policy_group.write_throughput
netapp_ontap.policy_group.other_data	netapp_ontap.policy_group.other_throughput
netapp_ontap.policy_group.total_data	netapp_ontap.policy_group.total_throughput
netapp_ontap.system_node.disk_data_read	netapp_ontap.system_node.disk_throughput_read
netapp_ontap.system_node.disk_data_written	netapp_ontap.system_node.disk_throughput_written
netapp_ontap.system_node.hdd_data_read	netapp_ontap.system_node.hdd_throughput_read
netapp_ontap.system_node.hdd_data_written	netapp_ontap.system_node.hdd_throughput_written
netapp_ontap.system_node.ssd_data_read	netapp_ontap.system_node.ssd_throughput_read
netapp_ontap.system_node.ssd_data_written	netapp_ontap.system_node.ssd_throughput_written
netapp_ontap.system_node.net_data_recv	netapp_ontap.system_node.net_throughput_recv
netapp_ontap.system_node.net_data_sent	netapp_ontap.system_node.net_throughput_sent
netapp_ontap.system_node.fcp_data_recv	netapp_ontap.system_node.fcp_throughput_recv
netapp_ontap.system_node.fcp_data_sent	netapp_ontap.system_node.fcp_throughput_sent
netapp_ontap.volume_node.cifs_read_data	netapp_ontap.volume_node.cifs_read_throughput
netapp_ontap.volume_node.cifs_write_data	netapp_ontap.volume_node.cifs_write_throughput
netapp_ontap.volume_node.nfs_read_data	netapp_ontap.volume_node.nfs_read_throughput
netapp_ontap.volume_node.nfs_write_data	netapp_ontap.volume_node.nfs_write_throughput
netapp_ontap.volume_node.iscsi_read_data	netapp_ontap.volume_node.iscsi_read_throughput
netapp_ontap.volume_node.iscsi_write_data	netapp_ontap.volume_node.iscsi_write_throughput
netapp_ontap.volume_node.fcp_read_data	netapp_ontap.volume_node.fcp_read_throughput
netapp_ontap.volume_node.fcp_write_data	netapp_ontap.volume_node.fcp_write_throughput
netapp_ontap.volume.read_data	netapp_ontap.volume.read_throughput
netapp_ontap.volume.write_data	netapp_ontap.volume.write_throughput

Previous Metric Name	New Metric Name
netapp_ontap.workload.read_data	netapp_ontap.workload.read_throughput
netapp_ontap.workload.write_data	netapp_ontap.workload.write_throughput
netapp_ontap.workload_volume.read_data	netapp_ontap.workload_volume.read_throughput
netapp_ontap.workload_volume.write_data	netapp_ontap.workload_volume.write_throughput

New Kubernetes Explorer

The [Kubernetes Explorer](#) provides a simple topology view of Kubernetes Clusters, allowing even non-experts to quickly identify issues & dependencies, from the cluster level down to the container and storage.

A wide variety of information can be explored using the Kubernetes Explorer's drill-down details for status, usage, and health of the Clusters, Nodes, Pods, Containers, and Storage in your Kubernetes environment.



December 2020

Simpler Kubernetes Installation

Kubernetes Agent installation has been streamlined to require fewer user interactions. [Installing the Kubernetes Agent](#) now includes Kubernetes data collection.

November 2020

Additional Dashboards

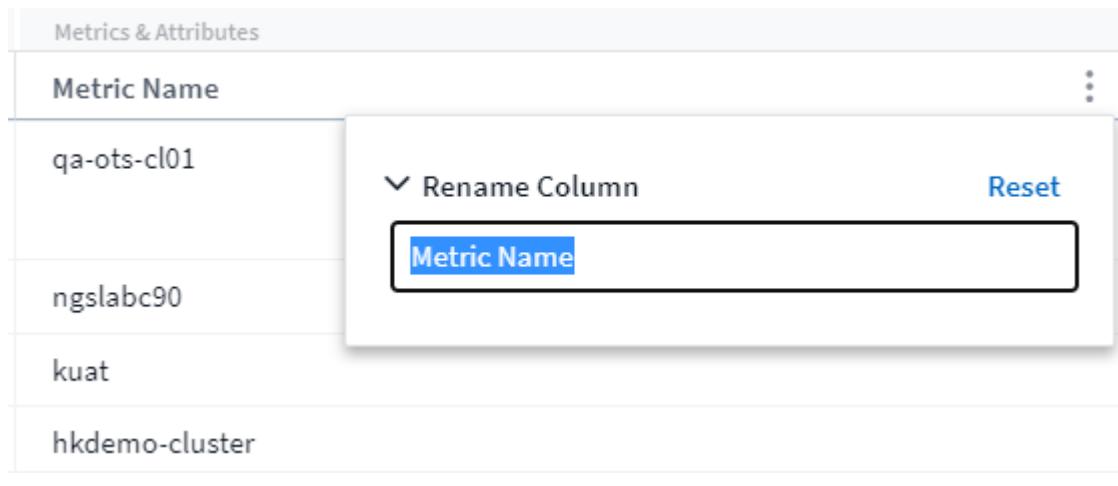
The following new ONTAP-focused dashboards have been added to the gallery and are available for import:

- ONTAP: Aggregate Performance & Capacity
- ONTAP FAS/AFF - Capacity Utilization
- ONTAP FAS/AFF - Cluster Capacity
- ONTAP FAS/AFF - Efficiency
- ONTAP FAS/AFF - FlexVol Performance
- ONTAP FAS/AFF - Node Operational/Optimal Points
- ONTAP FAS/AFF - PrePost Capacity Efficiencies
- ONTAP: Network Port Activity
- ONTAP: Node Protocols Performance
- ONTAP: Node Workload Performance (Frontend)
- ONTAP: Processor
- ONTAP: SVM Workload Performance (Frontend)
- ONTAP: Volume Workload Performance (Frontend)

Column Rename in Table Widgets

You can rename columns in the *Metrics and Attributes* section of a table widget by opening the widget in Edit mode and clicking the menu at the top of the column. Enter the new name and click *Save*, or click *Reset* to set the column back to the original name.

Note that this only affects the column's display name in the table widget; the metric/attribute name does not change in the underlying data itself.



October 2020

Default Expansion of Integration Data

Table widget grouping now allows for default expansions of Kubernetes, ONTAP Advanced Data, and Agent Node metrics. For example, if you group Kubernetes *Nodes* by *Cluster*, you will see a row in the table for each cluster. You could then expand each cluster row to see a list of the Node objects.

Basic Edition Technical Support

Technical Support is now available for subscribers to Cloud Insights Basic Edition in addition to Standard and Premium Editions. Additionally, Cloud Insights has simplified the workflow for creating a NetApp support ticket.

Cloud Secure Public API

Cloud Secure supports [REST APIs](#) for accessing Activity and Alert information. This is accomplished through the use of API Access Tokens, created through the Cloud Secure Admin UI, which are then used to access the REST APIs. Swagger documentation for these REST APIs is integrated with Cloud Secure.

September 2020

Query Page with Integration Data

The Cloud Insights Query page supports integration data (i.e. from Kubernetes, ONTAP Advanced Metrics, etc.). When working with integration data, the query results table displays a "Split-Screen" view, with object/grouping on the left side, and object data (attributes/metrics) on the right. You can also choose multiple attributes for grouping integration data.



The screenshot shows the Cloud Insights Query page interface. At the top, there is a search bar containing 'agent.node_fs' and a 'Filter By' button with a '+' icon. Below the search bar, there is a 'Group' section with two selected items: 'agent_node_name' and 'agent_node_os'. The main area displays a table titled '3 items found'. The table has three columns: 'Table Row Grouping', 'Metrics & Attributes', and a header row with 'agent_node_name', 'agent_node_os', 'free', and 'inodes_used'. The data rows are:

Table Row Grouping	Metrics & Attributes		
agent_node_name	agent_node_os	free	inodes_used
WIN2K12R2IMAGE	Microsoft Windows	70,594,338,816.00	0.00
WIN2K19IMAGE	Microsoft Windows	72,546,041,856.00	0.00
ci-q-a-chunge-qaa	Red Hat Enterprise Linux Server	169,010,801,322.67	21,844.00

Unit Display Formatting in Table Widget

Unit display formatting is now available in Table widgets for columns that display metric/counter data (for example, gigabytes, MB/second, etc.). To change a metric's display unit, click the "three dots" menu in the column header and select "Unit Display". You can choose from any of the available units. Available units will vary according to the type of metric data in the display column.

Table Widget

agent.node

Filter By: agent_node_name

8 items found

agent_node_name ↑	Metrics & Attributes
ci-qa-avinashp-k8-bakra-1	mem.used (GiB)
ci-qa-avinashp-k8-bakra-2	12.41
ci-qa-avinashp-k8-bakra-3	9.31
ci-qa-avinashp-k8-bakra-4	4.46
ci-qa-avinashp-k8-bakra-5	1.15
ci-qa-avinashp-k8wheel-1	15.23

Aggregation: byte (B)

Unit Display: gibibyte (GiB)

Cancel Save

Acquisition Unit Detail Page

Acquisition Units now have their own landing page, providing useful detail for each AU as well as information to help with troubleshooting. The [AU detail page](#) provides links to the AU's data collectors as well as helpful status information.

Cloud Secure Docker Dependency Removed

Cloud Secure's dependency on Docker has been removed. Docker is no longer required for Cloud Secure agent installation.

Reporting User Roles

If you have Cloud Insights Premium Edition with Reporting, every Cloud Insights user in your environment also has a Single Sign-On (SSO) login to the Reporting application (i.e. Cognos); by clicking the **Reports** link in the menu, they will automatically be logged in to Reporting.

Their user role in Cloud Insights determines their [Reporting user role](#):

Cloud Insights Role	Reporting Role	Reporting Permissions
Guest	Consumer	Can view, schedule, and run reports and set personal preferences such as those for languages and time zones. Consumers cannot create reports or perform administrative tasks.
User	Author	Can perform all Consumer functions as well as create and manage reports and dashboards.
Administrator	Administrator	Can perform all Author functions as well as all administrative tasks such configuration of reports and the shutdown and restart of reporting tasks.



Cloud Insights Reporting is available for environments of 500 MUs or more.



If you are a current Premium Edition customer and wish to retain your reports, read this [important note for existing customers](#).

New API Category for Data Ingestion

Cloud Insights has added a **Data Ingestion** API category, giving you greater control over custom data and agents. Detailed documentation for this and other API Categories can be found in Cloud Insights by navigating to **Admin > API Access** and clicking the *API Documentation* link. You can also attach a comment to the AU in the Note field, which is displayed on the AU detail page as well as the AU list page.

August 2020

Monitoring and Alerting

In addition to the current ability to set performance policies for storage objects, VMs, EC2, and ports, Cloud Insights Standard Edition now includes the ability to [configure monitors](#) for thresholds on Integration data for Kubernetes, ONTAP advanced metrics, and Telegraf plugins. You simply create a monitor for each object metric you want to trigger alerts, set the conditions for warning-level or critical-level thresholds, and specify the email recipient(s) desired for each level. You can then [view and manage alerts](#) to track trends or troubleshoot issues.



July 2020

Cloud Secure Take a Snapshot Action

Cloud Secure protects your data by automatically taking a snapshot when malicious activity is detected, ensuring that your data is safely backed up.

You can define automated response policies that take a snapshot when ransomware attack or other abnormal user activity is detected.

You can also take a snapshot manually from the alert page.

Automatic Snapshot taken:

Potential Attack Detail / Ransomware Attack

POTENTIAL ATTACK: AL_307
Ransomware Attack

Detected
4 days ago
Jul 26, 2020 3:38 AM

Action Taken
Snapshots Taken

Status
In Progress

Last snapshots taken by
Amit Schwartz
Jul 30, 2020 2:54 PM

How To:
Restore Entities

Re-Take Snapshots

Total Attack Results

1	0	5148
Affected Volumes	Deleted Files	Encrypted Files

5148 Files have been copied, deleted, and potentially encrypted by 1 user account.

This is potentially a sign of ransomware attack.
The extension "crypt" was added to each file.

Encrypted Files
Activity per minute

Related Users

	Ewen Hall Developer Engineering	5148 Encrypted Files	Detected 4 days ago Jul 26, 2020 3:38 AM	Action Taken Snapshots Taken
--	--	--------------------------------	---	--

Manual Snapshot:

Cloud Insights

MONITOR & OPTIMIZE Alerts / Nabilah Howell had an abnormal change in activity rate

CLOUD SECURE

ALERTS

FORENSICS

ADMIN

HELP

Jul 23, 2020 - Jul 26, 2020
1:44 AM 1:44 AM

WARNING: AL_306
Nabilah Howell had an abnormal change in activity rate.

Detected
5 days ago
Jul 25, 2020 1:44 PM

Action Taken
None

Status
New

Recommendation: Setup an Automated Response Policy
An Automated Response Policy will trigger measures to contain the damage automatically when a future attack is detected. Try it now.

Take Snapshots How To: Restore Entities

Nabilah Howell's Activity Rate Change

Typical	Alert
122.8 Activities Per Minute	210 Activities Per Minute
↑ 71%	

Nabilah Howell's activity rate grew 71% over their typical average.

Activity Rate
Activity per 5 minutes

Minimize

Metric/Counter updates

The following capacity counters are available for use in Cloud Insights UI and REST API. Previously these counters were only available for the Data Warehouse / Reporting.

Object Type	Counter
Storage	Capacity - Spare Raw Capacity - Failed Raw
Storage Pool	Data Capacity - Used Data Capacity - Total Other Capacity - Used Other Capacity - Total Capacity - Raw Capacity - Soft Limit
Internal Volume	Data Capacity - Used Data Capacity - Total Other Capacity - Used Other Capacity - Total Clone Saved Capacity - Total

Cloud Secure Potential Attack Detection

Cloud Secure now detects potential attacks such as ransomware. Click on an alert in the Alerts list page to open a detail page showing the following:

- Time of attack
- Associated user and file activity
- Action taken
- Additional information to assist with tracking down possible security breaches

Alerts page showing potential ransomware attack:



Detail page for potential ransomware attack:



POTENTIAL ATTACK: AL_305
Ransomware Attack

Detected
5 days ago
Jul 11, 2020 4:02 AM

Action Taken
None

Status
New

Total Attack Results

1 Affected Volumes | 0 Deleted Files | 4173 Encrypted Files

4173 Files have been copied, deleted, and potentially encrypted by 1 user account.

This is potentially a sign of ransomware attack.
The extension "crypt" was added to each file.

Encrypted Files

Activity per minute



Related Users



Kristjan Egilsson
Accountant
Finance

4173
Encrypted Files

Detected
5 days ago
Jul 11, 2020 4:02 AM

Action Taken
None



Username
us035

Email
Egilsson@netapp.com

Phone
387224312607

Department
Finance

Manager
Lyndsey Maddox

[View Activity Detail](#)

Top Activity Types
Activity per minute
Last access location: 10.197.144.115

Write Read Metadata Others



Subscribe to Premium Edition through AWS

During your trial of Cloud Insights, you can [self-subscribe](#) through AWS Marketplace to either Cloud Insights Standard Edition or Premium Edition. Previously, you could only self-subscribe through AWS Marketplace to Standard Edition only.

Enhanced Table Widget

The dashboard/asset page Table widget includes the following enhancements:

- "Split-Screen" view: Table widgets display the object/grouping on the left side, and the object data (attributes/metrics) on the right.

GroupBy All

Override Dashboard Time X

index_0.index_0 X

Filter By + Group agent_version X X ?

1 item found

Table Row Grouping		Metrics & Attributes				
agent_version		value	consumer	protocol_name	level0	level1
Java/1.8.0_242		1,649.80	CloudInsights	GENERATED	simulated	N/A

- Multiple attribute grouping: For Integration data (Kubernetes, ONTAP Advanced Metrics, Docker, etc.), you can choose multiple attributes for grouping. Data is displayed according to the grouping attributes/you choose.

Grouping with Integration Data (shown in Edit mode):

Table Widget - Integration Data Example

Override Dashboard Time Last 7 Days X

index_0.index_0 X

Filter By + Group agent_version X name X protocol_name X X ?

500 items found

Table Row Grouping			Metrics & Attributes				
agent_version	↑ name	protocol_name	value	consumer	protocol_name	level0	level1
Java/1.8.0_242	simulated.shinchaku-client-1010.counter.2...	GENERATED	1,597.16	CloudInsights	GENERATED	simulated	shinchaku-
Java/1.8.0_242	simulated.shinchaku-client-1008.counter.1...	GENERATED	1,604.92	CloudInsights	GENERATED	simulated	shinchaku-
Java/1.8.0_242	simulated.shinchaku-client-1015.counter.1...	GENERATED	1,684.82	CloudInsights	GENERATED	simulated	shinchaku-
Java/1.8.0_242	simulated.shinchaku-client-1008.counter.0...	GENERATED	1,677.15	CloudInsights	GENERATED	simulated	shinchaku-

Cancel Save

- Grouping for Infrastructure data (storage, EC2, VM, ports, etc.) is by a single attribute as before. When grouping by an attribute which is not the object, the table will allow you to expand the group row to see all the objects within the group.

Grouping with Infrastructure data (shown in display mode):

GroupBy Date

⌚ 1h

4 items found in 2 groups

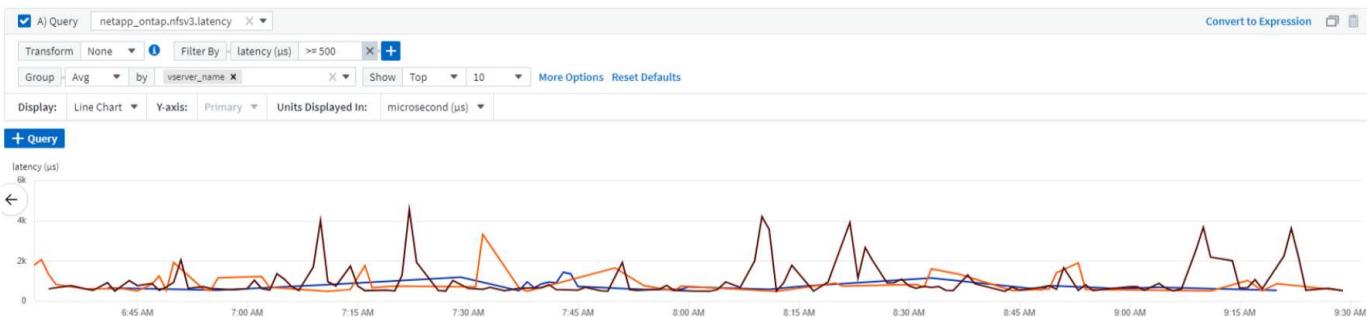
Active Date	Storage Node	Cache Hit Ratio - Total (%)	IOPS - Total (IO...)	IOPS - Write (I...)	Latency
06/01/2020 (1)	ocinaneqa1-01	N/A	N/A	N/A	N/A
06/01/2020	ocinaneqa1-01	N/A	N/A	N/A	N/A
■ N/A (3)	--	N/A	N/A	N/A	N/A

Metrics Filtering

In addition to filtering on an object's attributes in a widget, you can now filter on metrics as well.



When working with integration data (Kubernetes, ONTAP Advanced Data, etc.), metric filtering removes the individual/unmatched data points from the plotted data series, unlike infrastructure data (storage, VM, ports etc.) where filters work on the aggregated value of the data series and potentially remove the entire object from the chart.



ONTAP Advanced Counter Data

Cloud Insights takes advantage of NetApp's ONTAP-specific **Advanced Counter Data**, which provides a host of counters and metrics collected from ONTAP devices. ONTAP Advanced Counter Data is available to all NetApp ONTAP customers. These metrics enable customized and wide-ranging visualization in Cloud Insights widgets and dashboards.

ONTAP Advanced Counters can be found by searching for "netapp_ontap" in the widget's query, and selecting from among the counters.



You can refine your search by typing additional parts of the counter name. For example:

- *lif*
- *aggregate*
- *offbox_vscan_server*
- and more



Please note the following:

- Advanced Data collection will be enabled by default for new ONTAP data collectors. To enable Advanced Data collection for your existing ONTAP data collectors, edit the data collector and expand the *Advanced Configuration* section.
- Advanced Data collection is not available for 7-mode ONTAP.

Advanced Counter Dashboards

Cloud Insights comes with a variety of pre-designed dashboards to help get you started on visualizing ONTAP Advanced Counters for topics such as *Aggregate Performance*, *Volume Workload*, *Processor Activity*, and more. If you have at least one ONTAP data collector configured, these can be imported from the Dashboard Gallery on any dashboard list page.

Learn More

More information on ONTAP Advanced Data can be found at the following links:

- <https://mysupport.netapp.com/site/tools/tool-eula/netapp-harvest> (Note: You will need to sign in to NetApp Support)
- <https://nabox.org/faq/>

Policies and Violations Menu

Performance Policies and Violations are now found under the **Alerts** menu. Policy and Violation functionality are unchanged.



Updated Telegraf Agent

The agent for ingestion of telegraf integration data has been updated to [version 1.14](#), which includes bugs fixes, security fixes, and new plugins.

Note: When configuring a Kubernetes data collector on the Kubernetes platform, you may see an "HTTP status 403 Forbidden" error in the log, due to insufficient permissions in the "clusterrole" attribute.

To work around this issue, add the following highlighted lines to the *rules:* section of the endpoint-access clusterrole, and then restart the Telegraf pods.

```

rules:
- apiGroups:
  - ""
  - apps
  - autoscaling
  - batch
  - extensions
  - policy
  - rbac.authorization.k8s.io
attributeRestrictions: null
resources:
- nodes/metrics
- nodes/proxy      <== Add this line
- nodes/stats
- pods            <== Add this line
verbs:
- get
- list           <== Add this line

```

June 2020

Simplified Data Collector Error Reporting

Reporting a data collector error is easier with the *Send Error Report* button on the data collector page. Clicking the button sends basic information about the error to NetApp and prompts investigation into the problem. Once pressed, Cloud Insights acknowledges that NetApp has been notified, and the Error Report button is disabled to indicate that an error report for that data collector has been sent. The button remains disabled until the browser page is refreshed.



Widget Improvements

The following improvements have been made in dashboard widgets. These improvements are considered Preview functionality and may not be available for all Cloud Insights environments.

- New object/metric chooser: Objects (Storage, Disk, Ports, Nodes, etc.) and their associated metrics (IOPS, Latency, CPU Count, etc.) are now available in widgets in a single inclusive drop-down with powerful search capability. You can enter multiple partial terms in the drop-down, and Cloud Insights will list all object metrics meeting those terms.



- Multiple tags grouping: When working with integration data (Kubernetes, etc.), you may group the data by multiple tags/attributes. For example, Sum memory usage by Kubernetes Namespace and Container name.



May 2020

Reporting User Roles

The following roles have been added for Reporting:

- Cloud Insights Consumers: can run and view reports
- Cloud Insights Authors: can perform the Consumer functions as well as create and manage reports and dashboards
- Cloud Insights Administrators: can perform the Author functions as well as all administrative tasks

Cloud Secure Updates

Cloud Insights includes the following recent Cloud Secure changes.

In the Forensics > Activity Forensics page, we provide two views to analyze and investigate user activity:

- Activity view, focused on user activity (What operation? Where performed?)
- Entities view, focused on what files the user accessed.



Additionally, the Alert email notification now contains a direct link to the alert page.

Dashboard Grouping

Dashboard grouping allows better [management of dashboards](#) that are relevant to you. You can add related dashboards to a group for "one-stop" management of, for example, your storage or virtual machines.

Groups are customized per user, so one person's groups can be different from someone else's. You can have as many groups as you need, with as few or as many dashboards in each group as you like.

Dashboard Groups (3)

All Dashboards (60)

My Dashboards (11)

Storage Group (7)

Dashboards (7)

<input type="checkbox"/>	Name ↑
	Dashboard - Storage Cost
	Dashboard - Storage IO Detail
	Dashboard - Storage Overview
	Gauges Storage Performance
	Storage Admin - Which nodes are in high demand?
	Storage Admin - Which pools are in high demand?
	Storage IOPs

Dashboard Pinning

You can pin dashboards so favorites always appear at the top of the list.

Dashboards (7)

<input type="checkbox"/>	Name ↑
<input checked="" type="checkbox"/>	Dashboard - Storage Overview
<input checked="" type="checkbox"/>	Storage Admin - Which nodes are in high demand?
<input checked="" type="checkbox"/>	Storage IOPs
	Dashboard - Storage Cost
	Dashboard - Storage IO Detail
	Gauges Storage Performance
	Storage Admin - Which pools are in high demand?

TV Mode and Auto-Refresh

[TV Mode and Auto-Refresh](#) allow for near-real-time display of data on a dashboard or asset page:

- **TV Mode** provides an uncluttered display; the navigation menu is hidden, providing more screen real estate for your data display.
- Data in widgets on Dashboards and Asset Landing Pages **Auto-Refresh** according a refresh interval (as little as every 10 seconds) determined by the Dashboard Time Range selected (or widget time range, if set to override the dashboard time).

Combined, TV Mode and Auto-Refresh provide a live view of your Cloud Insights data, perfect for seamless demonstrations or in-house monitoring.

April 2020

New Dashboard Time Range Choices

Time range choices for dashboards and other Cloud insights pages now include *Last 1 Hour* and *Last 15 Minutes*.

Cloud Secure Updates

Cloud Insights includes the following recent Cloud Secure changes.

- Better file and folder metadata change recognition to detect if the user changed Permission, Owner, or Group Ownership.
- Export user activity report to CSV.

Cloud Secure monitors and audits all user access operations on files and folders. Activity auditing allows you to comply with internal security policies, meet external compliance requirements such as PCI, GDPR, and HIPAA, and conduct data breach and security incident investigations.

Default Dashboard Time

The default time range for dashboards is now 3 Hours instead of 24 hours.

Optimized Aggregation Times

Optimized [time aggregation](#) intervals in time-series widgets (Line, Spline, Area, and Stacked Area charts) are more frequent for 3-hour and 24-hour dashboard/widget time ranges, allowing for faster charting of data.

- 3 hour time range optimizes to a 1 minute aggregation interval. Previously this was 5 minutes.
- 24 hour time range optimizes to a 30 minute aggregation interval. Previously this was 1 hour.

You can still override the optimized aggregation by setting a custom interval.

Display Unit Auto-Format

In most widgets, Cloud Insights knows the base unit in which to display values, for example *Megabytes*, *Thousands*, *Percentage*, *Milliseconds (ms)*, etc., and now [automatically formats](#) the widget to the most readable unit. For example a data value of 1,234,567,890 bytes would be auto formatted to 1.23 gibabytes. In many cases, Cloud Insights knows the best format for the data being acquired. In cases where the best format is not known, or in widgets where you want to override the automatic formatting, you can choose the format you want.



Import Annotations Using API

With Cloud Insights Premium Edition's powerful API, you can now [import annotations](#) and assign them to objects using a .CSV file. You can also import applications and assign business entities in the same way.

ASSETS.import

PUT /assets/import Import assets from a CSV file.

Import annotations and applications from the given CSV file. The format of the CSV file is following:

```

, <Annotation Type> [, <Annotation Type> ...] [, Application] [, Tenant] [, Line_Of_Business] [, Business_Unit] [, Project]
<Object Type Value 1>, <Object Name or Key 1>, <Annotation Value> [, <Annotation Value> ...] [, <Application>] [, <Tenant>] [, <Line_Of_Business>] [, <Business_Unit>] [, <Project>]
<Object Type Value 2>, <Object Name or Key 2>, <Annotation Value> [, <Annotation Value> ...] [, <Application>] [, <Tenant>] [, <Line_Of_Business>] [, <Business_Unit>] [, <Project>]
<Object Type Value 3>, <Object Name or Key 3>, <Annotation Value> [, <Annotation Value> ...] [, <Application>] [, <Tenant>] [, <Line_Of_Business>] [, <Business_Unit>] [, <Project>]
...
<Object Type Value N>, <Object Name or Key N>, <Annotation Value> [, <Annotation Value> ...] [, <Application>] [, <Tenant>] [, <Line_Of_Business>] [, <Business_Unit>] [, <Project>]

```

Simpler Widget Selector

Adding widgets to dashboards and asset landing pages is easier with a new widget selector that shows all widget types in a single all-at-once view, so the user no longer needs to scroll through a list of widget types to find the one they want to add. Related widgets are color-coordinated and grouped by proximity in the new selector.



February 2020

API with Premium Edition

Cloud Insights Premium Edition comes with a [powerful API](#) that can be used to integrate Cloud Insights with other applications, such as CMDB's or other ticketing systems.

Detailed, Swagger-based information is found in **Admin > API Access**, under the **API Documentation** link. Swagger provides a brief description and usage information for the API, and allows you to try each API out in your environment.

The Cloud Insights API uses Access Tokens to provide permission-based access to categories of API, such as ASSETS or COLLECTION.

NetApp / Admin / API Access

Choose API Documentation type:

- Getting Started
- All Categories
- Assets
- Data Collection
- Data Ingestion
- Data Warehouse

API Documentation ▾ X

Initial Polling After Adding A Data Collector

Previously, after configuring a new data collector, Cloud Insights would poll the data collector immediately to gather *inventory* data, but would wait until the configured performance poll interval (typically 15 minutes) to gather initial *performance* data. It would then wait for another interval before initiating the second performance

poll, which meant it would take up to *30 minutes* before meaningful data was acquired from a new data collector.

Data collector [polling](#) has been greatly improved, such that the initial performance poll occurs immediately after the inventory poll, with the second performance poll occurring within a few seconds after completion of the first performance poll. This allows Cloud Insights to begin showing useful data on dashboards and graphs within a very short time.

This poll behavior also occurs after editing the configuration of an existing data collector.

Easier Widget Duplication

It is easier than ever to create a copy of a widget on a dashboard or landing page. In dashboard Edit mode, click the menu on the widget and select **Duplicate**. The widget editor is launched, pre-filled with the original widget's configuration and with a "copy" suffix in the widget name. You can easily make any necessary changes and Save the new widget. The widget will be placed at the bottom of your dashboard, and you can position it as needed. Remember to Save your dashboard when all changes are complete.



Single Sign-On (SSO)

With Cloud Insights Premium Edition, administrators can enable [Single Sign-On \(SSO\)](#) access to Cloud Insights for all users in their corporate domain, without having to invite them individually. With SSO enabled, any user with the same domain email address can log into Cloud Insights using their corporate credentials.



SSO is only available in Cloud Insights Premium Edition, and must be configured before it can be enabled for Cloud Insights. SSO configuration includes [Identity Federation](#) through NetApp Cloud Central. Federation allows single sign-on users to access your NetApp Cloud Central accounts using credentials from your corporate directory.

January 2020

Swagger documentation for REST API

Swagger explains each available REST API in Cloud Insights, as well as its usage and syntax. Information on Cloud Insights APIs is available in [documentation](#).

Feature Tutorials Progress Bar

The feature tutorials checklist has been moved to the top banner and now features a progress indicator. Tutorials are available for each user until dismissed, and are always available in Cloud Insights [documentation](#).



Acquisition Unit Changes

When installing an Acquisition Unit (AU) on a host or VM that has the same name as an already-installed AU, Cloud Insights assures a unique name by appending the AU name with "_1", "_2", etc. This is also the case when uninstalling and reinstalling an AU from the same VM without first removing it from Cloud Insights. Want a different AU name altogether? No problem; AU's can be renamed after installation.

Optimized Time Aggregation in Widgets

In widgets, you can choose between an *Optimized* time aggregation interval or a *Custom* interval that you set. Optimized aggregation automatically selects the right time interval based on the selected dashboard time range (or widget time range, if overriding the dashboard time). The interval dynamically changes as the dashboard or widget time range is changed.

Simplified "Getting Started with Cloud Insights" process

The process for getting started using Cloud Insights has been simplified to make your first-time setup smoother and easier. Simply select an initial data collector and follow the instructions. Cloud Insights will walk you through configuring the data collector and any agent or acquisition unit required. In most cases it will even import one or more initial dashboards so you can start gaining insight into your environment quickly (but please allow up to 30 minutes for Cloud Insights to collect meaningful data).

Additional improvements:

- Acquisition Unit installation is simpler and runs faster.
- Alphabetical Data Collectors choices make it easier to find the one you're looking for.
- Improved Data Collector setup instructions are easier to follow.
- Experienced users can skip the getting started process with the click of a button.
- A new Progress bar shows you where you are in the process.



Select a Data Collector

Install Agent

Configure Collector

December 2019

Business Entity can be used in filters

Business Entity annotations can be used in filters for queries, widgets, performance policies, and landing pages.

Drill-down available for Single-Value and Gauge widgets, and any widgets rolled to by "All"

Clicking the value in a single-value or gauge widget opens a query page showing the results of the first query used in the widget. Additionally, clicking the legend for any widget whose data is rolled up by "All" will also open a query page showing the results of the first query used in the widget.

Trial period extended

New users who sign up for a free trial of Cloud Insights now have 30 days to evaluate the product. This is an increase from the previous 14-day trial period.

Managed Unit calculation

The calculation of Managed Units (MUs) in Cloud Insights has been changed to the following:

- 1 Managed Unit = 2 hosts (any virtual or physical machine)
- 1 Managed Unit = 4 TB of unformatted capacity of physical or virtual disks

This change effectively doubles the environment capacity that you can monitor using your existing Cloud Insights subscription.

November 2019

Editions Feature Comparison Table

The **Admin > Subscription** page [comparison table](#) has been updated to list the feature sets available in Basic, Standard, and Premium Editions of Cloud Insights. NetApp is constantly improving its Cloud Services, so check this page often to find the Edition that's right for your evolving business needs.

October 2019

Reporting

Cloud Insights Reporting is a business intelligence tool that enables you to view pre-defined reports or create custom reports. With Reporting you can perform the following tasks:

- Run a pre-defined report
- Create a custom report
- Customize the report format and delivery method
- Schedule reports to run automatically
- Email reports
- Use colors to represent thresholds on data

Cloud Insights Reporting can generate custom reports for areas like chargeback, consumption analysis, and forecasting, and can help answer questions such as the following:

- What inventory do I have?
- Where is my inventory?
- Who is using our assets?
- What is the chargeback for allocated storage for a business unit?
- How long until I need to acquire additional storage capacity?
- Are business units aligned along the proper storage tiers?
- How is storage allocation changing over a month, quarter, or year?

Reporting is available with Cloud Insights **Premium Edition**.

Active IQ Enhancements

Active IQ Risks are now available as objects that can be queried as well as used in dashboard table widgets. The following Risks object attributes are included:

- * Category
- * Mitigation Category
- * Potential Impact
- * Risk Detail
- * Severity
- * Source
- * Storage
- * Storage Node
- * UI Category

September 2019

New Gauge Widgets

Two new widgets are available for displaying single-value data on your dashboards in eye-catching colors based on thresholds you specify. You can display values using either a **Solid Gauge** or **Bullet Gauge**. Values that land inside the Warning range are displayed in orange. Values in the Critical range are displayed in red. Values below the Warning threshold are displayed in green.



Conditional Color Formatting for Single Value Widget

You can now display the Single-Value widget with a colored background based on thresholds you set.



Invite Users During Onboarding

At any point during the onboarding process, you can click on Admin > User Management > +User to invite additional users to your Cloud Insights environment. Be aware that users with *Guest* or *User* roles will see greater benefit once onboarding is complete and data has been collected.

Data Collector Detail Page improvement

The data collector detail page has been improved to display errors in a more readable format. Errors are now displayed in a separate table on the page, with each error displayed on a separate line in the case of multiple

errors for the data collector.

August 2019

All vs. Available Data Collectors

When adding data collectors to your environment, you can set a filter to show only the data collectors available to you based on your subscription level, or all data collectors.

ActiveIQ Integration

Cloud Insights collects data from NetApp ActiveIQ, which provides a series of visualizations, analytics, and other support related services to NetApp customers and their hardware / software systems. Cloud Insights integrates with ONTAP Data Management systems. See [Active IQ](#) for more information.

July 2019

Dashboard Improvements

Dashboards and Widgets have been improved with the following changes:

- In addition to Sum, Min, Max, and Avg, **Count** is now an option for roll up in Single-Value widgets. When rolling up by “Count”, Cloud Insights checks if an object is active or not, and only adds the active ones to the count. The resulting number is subject to aggregation and filters.
- In the Single-Value widget, you now have a choice to display the resulting number with 0, 1, 2, 3, or 4 decimal places.
- Line charts show an axis label and units when a single counter is being plotted.
- **Transform** option is available for Services integration data now in all time-series widgets for all metrics. For any services integration (Telegraf) counter or metric in time-series widgets (Line, Spline, Area, Stacked Area), you are given a choice of how you want to [Transform the values](#). None (display value as-is), Sum, Delta, Cumulative, etc.

Downgrading to Basic Edition

Downgrade to Basic Edition fails with an error message if there is no available NetApp device configured that has successfully completed a poll in the last 7 days.

Collecting Kube-State-Metrics

The [Kubernetes Data Collector](#) now collects objects and counters from the kube-state-metrics plugin, greatly expanding the number and scope of metrics available for monitoring in Cloud Insights.

June 2019

Cloud Insights Editions

Cloud Insights is available in different Editions to fit your budget and business needs. Existing NetApp customers with an active NetApp support account can enjoy 7 days of data retention and access to NetApp data collectors with the free **Basic Edition**, or get increased data retention, access to all supported data collectors, expert technical support and more with **Standard Edition**. For more information on available features, see NetApp's [Cloud Insights](#) site.

New Infrastructure Data Collector: NetApp HCI

- [NetApp HCI Virtual Center](#) has been added as an Infrastructure data collector. The HCI Virtual Center data collector collects NetApp HCI Host information and requires read-only privileges on all objects within the Virtual Center.

Note that the HCI data collector acquires from the HCI Virtual Center only. To collect data from the storage system, you must also configure the NetApp [SolidFire](#) data collector.

May 2019

New Service Data Collector: Kapacitor

- [Kapacitor](#) has been added as a data collector for services.

Integration with Services via Telegraf

In addition to acquisition of data from infrastructure devices such as switches and storage, Cloud Insights now collects data from a variety of Operating Systems and Services, using [Telegraf as its agent](#) for collection of integration data. Telegraf is a plugin-driven agent that can be used to collect and report metrics. Input plugins are used to collect the desired information into the agent by accessing the system/OS directly, by calling third-party APIs, or by listening to configured streams.

Documentation for currently supported integrations can be found in the menu to the left under [Reference and Support](#).

Storage Virtual Machine Assets

- Storage Virtual Machines (SVMs) are available as assets in Cloud Insights. SVMs have their own Asset Landing Pages, and can be displayed and used in searches, queries, and filters. SVMs can also be used in dashboard widgets as well as associated with annotations.

Reduced Acquisition Unit System Requirements

- The system CPU and memory requirements for the Acquisition Unit (AU) software have been reduced. The new requirements are:

Component	Old Requirement	New Requirement
CPU Cores	4	2

Memory	16 GB	8 GB
--------	-------	------

Additional Platforms Supported

- The following platforms have been added to those currently [supported for Cloud Insights](#):

Linux	Windows
CentOS 7.3 64-bit	Microsoft Windows 10 64-bit
CentOS 7.4 64-bit	Microsoft Windows Server 2008 R2
CentOS 7.6 64-bit	Microsoft Windows Server 2019
Debian 9 64-bit	
Red Hat Enterprise Linux 7.3 64-bit	
Red Hat Enterprise Linux 7.4 64-bit	
Red Hat Enterprise Linux 7.6 64-bit	
Ubuntu Server 18.04 LTS	

April 2019

Filter Virtual Machines by Tags

When configuring the following data collectors, you can filter to include or exclude virtual machines from data collection according to their Tags or Labels.

- [Amazon EC2](#)
- [Azure](#)
- [Google Cloud Platform](#)

March 2019

Email Notifications for Subscription-related Events

- You can select recipients for email [notifications](#) when subscription-related events occur, such as upcoming trial expiration or subscribed account changes. You can choose recipients for these notifications from among following:
 - All Account Owners
 - All Administrators
 - Additional Email Addresses that you specify

Additional Dashboards

- The following new AWS-focused [dashboards](#) have been added to the gallery and are available for import:
 - AWS Admin - Which EC2 are in high demand?
 - AWS EC2 Instance Performance by Region

February 2019

Collecting from AWS Child Accounts

- Cloud Insights supports [collection from AWS child accounts](#) within a single data collector. Your AWS environment must be configured to allow Cloud Insights to collect from child accounts.

Data Collector Naming

- Data Collector names can now include periods (.), hyphens (-), and spaces () in addition to letters, numbers, and underscores. Names may not begin or end with a space, period, or hyphen.

Acquisition Unit for Windows

- You can configure a Cloud Insights Acquisition Unit on a Windows server/VM. Review the Windows [prerequisites](#) before installing the [Acquisition Unit software](#).

January 2019

"Owner" field is more readable

- In Dashboard and Query lists, the data for the "Owner" field was previously an authorization ID string, instead of a user-friendly owner name. The "Owner" field now shows a simpler and more readable owner name.

Managed Unit Breakdown on Subscription Page

- For each data collector listed on the [Admin > Subscription](#) page, you can now see a breakdown of Managed Unit (MU) counts for hosts and storage, as well as the total.

December 2018

Improvement of UI Load Time

- The initial loading time for the Cloud Insights user interface (UI) has been significantly improved. Refresh time for the UI also benefits from this improvement in circumstances where metadata is loaded.

Bulk Edit Data Collectors

- You can edit information for multiple data collectors at the same time. On the [Admin > Data Collectors](#) page, select the data collectors to modify by checking the box to the left of each and click the **Bulk Actions** button. Choose **Edit** and modify the necessary fields.

The data collectors selected must be the same vendor and model, and reside on the same Acquisition Unit.

Support and Subscription pages are Available During Onboarding

- During the onboarding workflow, you can navigate to the **Help > Support** and **Admin > Subscription** pages. Returning from those pages returns you to the onboarding workflow, providing you have not closed the browser tab.
-

November 2018

Subscribe through NetApp Sales or AWS Marketplace

- Cloud Insights subscription and billing is now available directly through NetApp. This is in addition to the self-serve subscription available through AWS Marketplace. A new **Contact Sales** link is presented on the **Admin > Subscription** page. For customers whose environments have or are expected to have 1,000 or more Managed Units (MUs), it is recommended to contact NetApp sales via the Contact Sales link.

Text Annotation Hyperlinks

- Text-type annotations can now include hyperlinks.

Onboarding Walkthrough

- Cloud Insights now features an onboarding walkthrough for the first user (administrator or account owner) to log in to a new environment. The walkthrough takes you through installing an Acquisition Unit, configuring an initial data collector, and selecting one or more useful dashboards.

Import Dashboards from the Gallery

- In addition to selecting dashboards during onboarding, you can import dashboards via **Dashboards > Show All Dashboards** and clicking **+From Gallery**.

Duplicating Dashboards

- The ability to duplicate a dashboard has been added to the dashboard list page as a choice in the options menu for each dashboard, and on a dashboard's main page itself from the Save menu.

Cloud Central products menu

- The menu allowing you to switch to other NetApp Cloud Central products has moved to the upper right corner of the screen.

Cloud Insights Onboarding

Before you can start working with Cloud Insights, you must sign up on the **NetApp Cloud Central** portal. If you already have a NetApp Cloud Central login, you can start a free trial of Cloud Insights with a few quick steps.

Creating your NetApp Cloud Central account

To sign up for access to NetApp's cloud services, go to [NetApp Cloud Central](#) and click **Sign Up**.

- Enter a valid business email address and choose a password.
- Enter your company name, and your full name.
- Accept the terms and conditions and click **Sign Up**.

You will then be taken to NetApp's cloud offerings page.

Select Cloud Insights.

What if I already have a NetApp Cloud login?

If you already have a NetApp Cloud Central account, simply choose **Log In** on the [NetApp Cloud Central](#) portal page.

Enter your email address and password. You will then be taken to NetApp's cloud offerings page.

Select Cloud Insights.

Starting your Cloud Insights free trial

If this is your first time logging in to Cloud Insights, under the Cloud Insights offering, click on **Start Free Trial**. Cloud Insights will then create your company's environment.

Once the creation of your environment is complete, you can use your Cloud Central credentials to log in and start your free, 30-day trial of Cloud Insights. During this trial you can explore all the features that Cloud Insights Standard Edition has to offer.

During the free trial, you can [start your subscription](#) to Cloud Insights at any time. When you are subscribed, You can use the Cloud Insights features based on your current subscription.

Sign in and go

Once your environment has been created, at any time you can simply log in to the NetApp Cloud Portal and click **Go to Cloud Insights**. You will be taken directly to your Cloud Insights environment.

You can also open a browser directly to your Cloud Insights environment URL, for example:

```
https://<environment-prefix>.c01.cloudinsights.netapp.com/
```

The URL will also be included in each user's invitation email for simple access and bookmarking. If the user is

not already logged in to Cloud Central, they will be prompted to log in.



New users must still sign up for access to Cloud Central before they can access their environment URL.

The first time you log in to a new environment, you will be guided through setting up to [begin gathering data](#).

Logging Out

To log out of Cloud Insights, click your **User Name** and select **Log Out**. You will be taken back to the Cloud Central sign in screen.



Logging out of Cloud Insights logs you out of Cloud Central. You will also be logged out of other NetApp Cloud services that use the Cloud Central sign-in.

Security

Cloud Insights Security

Product and customer data security is of utmost importance at NetApp. Cloud Insights follows security best practices throughout the release life cycle to make sure customer information and data is secured in the best possible way.

Security Overview

Physical security

The Cloud Insights production infrastructure is hosted in Amazon Web Services (AWS). Physical and environmental security-related controls for Cloud Insights production servers, which include buildings as well as locks or keys used on doors, are managed by AWS. As per AWS: "Physical access is controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff utilize multi-factor authentication mechanisms to access data center floors."

Cloud Insights follows the best practices of the [Shared Responsibility model](#) described by AWS.

Product security

Cloud Insights follows a development lifecycle in line with Agile principles, thus allowing us to address any security-oriented software defects more rapidly, compared to longer release cycle development methodologies. Using continuous integration methodologies, we are able to rapidly respond to both functional and security changes. The change management procedures and policies define when and how changes occur and help to maintain the stability of the production environment. Any impactful changes are formally communicated, coordinated, properly reviewed, and approved prior to their release into the production environment.

Network security

Network access to resources in the Cloud Insights environment is controlled by host-based firewalls. Each resource (such as a load balancer or virtual machine instance) has a host-based firewall that restricts inbound traffic to only the ports needed for that resource to perform its function.

Cloud Insights uses various mechanisms including intrusion detection services to monitor the production environment for security anomalies.

Risk Assessment

Cloud Insights team follows a formalized Risk Assessment process to provide a systematic, repeatable way to identify and assess the risks so that they can be appropriately managed through a Risk Treatment Plan.

Data protection

The Cloud Insights production environment is set up in a highly redundant infrastructure utilizing multiple availability zones for all services and components. Along with utilizing a highly available and redundant compute infrastructure, critical data is backed up at regular intervals and restores are periodically tested. Formal backup policies and procedures minimize the impact of interruptions of business activities and protects business processes against the effects of failures of information systems or disasters and ensures their timely and adequate resumption.

Authentication and access management

All customer access to Cloud Insights is done via browser UI interactions over https. Authentication is accomplished via the 3rd party service, Auth0. NetApp has centralized on this as the authentication layer for all Cloud Data services.

Cloud Insights follows industry best practices including “Least Privilege” and “Role-based access control” around logical access to the Cloud Insights production environment. Access is controlled on a strict need basis and is only granted for select authorized personnel using multi-factor authentication mechanisms.

Collection and protection of customer data

All customer data is encrypted in transit across public networks and encrypted at rest. Cloud Insights utilizes encryption at various points in the system to protect customer data using technologies that includes Transport Layer Security (TLS) and the industry-standard AES-256 algorithm.

Customer deprovisioning

Email notifications are sent out at various intervals to inform the customer their subscription is expiring. Once the subscription has expired, the UI is restricted and a grace period begins for data collection. The customer is then notified via email. Trial subscriptions have a 14-day grace period and paid subscription accounts have a 28-day grace period. After the grace period has expired, the customer is notified via email that the account will be deleted in 2 days. A paid customer can also request directly to be off the service.

Expired tenants and all associated customer data are deleted by the Cloud Insights Operations (SRE) team at the end of the grace period or upon confirmation of a customer’s request to terminate their account. In either case, the SRE team runs an API call to delete the account. The API call deletes the tenant instance and all customer data. Customer deletion is verified by calling the same API and verifying that the customer tenant status is “DELETED.”

Security incident management

Cloud Insights is integrated with NetApp’s Product Security Incident Response Team (PSIRT) process to find, assess, and resolve known vulnerabilities. PSIRT intakes vulnerability information from multiple channels including customer reports, internal engineering, and widely recognized sources such as the CVE database.

If an issue is detected by the Cloud Insights engineering team, the team will initiate the PSIRT process, assess, and potentially remediate the issue.

It is also possible that a Cloud Insights customer or researcher may identify a security issue with the Cloud Insights product and report the issue to Technical Support or directly to NetApp’s incident response team. In these cases, the Cloud Insights team will initiate the PSIRT process, assess, and potentially remediate the issue.

Vulnerability and Penetration testing

Cloud Insights follows industry best practices and performs regular vulnerability and penetration testing using internal and external security professionals and companies.

Security awareness training

All Cloud Insights personnel undergo security training, developed for individual roles, to make sure each employee is equipped to handle the specific security-oriented challenges of their roles.

Compliance

Cloud Insights performs independent third-party Audit and validations from external Licensed CPA firm of its security, processes, and services, including completion of the SOC 2 Audit.

Information and Region

NetApp takes the security of customer information very seriously. Here is how and where Cloud Insights stores your information.

What information does Cloud Insights store?

Cloud Insights stores the following information:

- Performance data

Performance data is time-series data providing information about the performance of the monitored device/source. This includes, for example, the number of IOs delivered by a storage system, the throughput of a FibreChannel port, the number of pages delivered by a web server, the response time of a database, and more.

- Inventory data

Inventory data consists of metadata describing the monitored device/source and how it is configured. This includes, for example, hardware and software versions installed, disks and LUNs in a storage system, CPU cores, RAM and disks of a virtual machine, the tablespaces of a database, the number and type of ports on a SAN switch, directory/file names (if Storage Workload Security is enabled), etc.

- Configuration data

This summarizes customer-provided configuration data used to manage customer inventory and operations, e.g. hostnames or IP addresses of the monitored devices, polling intervals, timeout values, etc.

- Secrets

Secrets consist of the credentials used by the Cloud Insights Acquisition Unit to access customer devices and services. These credentials are encrypted using AES-256, and the private keys are stored only on the Acquisition Units and never leave the customer environment. Even privileged Cloud Insights SREs are unable to access customer secrets in plain-text due to this design.

- Functional Data

This is data generated as a result of NetApp providing the Cloud Data Service, which informs NetApp in the development, deployment, operations, maintenance, and securing of the Cloud Data Service. Functional Data does not contain Customer Information or Personal Information.

- User Access data

Authentication and access information that allows NetApp Cloud Central to communicate with regional Cloud Insights sites, including data related to user Authorization.

- Storage Workload Security User Directory Data

In cases where the Workload Security functionality is enabled AND the customer chooses to enable the

User Directory collector, the system will store user display names, corporate email addresses, and other information collected from Active Directory.



User Directory data refers to user directory information collected by the Workload Security User Directory data collector, not to data about the users of Cloud Insights/Workload Security themselves.

No explicit personal data is collected from infrastructure and services resources. Collected information consists of performance metrics, configuration information and infrastructure metadata only, much like many vendor phone-homes, including NetApp auto-support and ActiveIQ. However, depending on a customer's naming conventions, data for shares, volumes, VMs, qtrees, applications, etc. may contain personally identifiable information.

If Workload Security is enabled, the system additionally looks at file and directory names on SMB or other shares, which may contain personally identifiable information. Where customers enable the Workload Security User Directory Collector (which essentially maps Windows SIDs to usernames through Active Directory), the display name, corporate email address and any additional attributes selected will be collected and stored by Cloud Insights.

Additionally, access logs to Cloud Insights are maintained and contain users' IP and email addresses used to log into the service.

Where is my information stored?

Cloud Insights stores information according to the region in which your environment is created.

The following information is stored in the host region:

- Telemetry and asset/object information, including counters and performance metrics
- Acquisition Unit information
- Functional data
- Audit information on user activities inside Cloud Insights
- Workload Security Active Directory information
- Workload Security Audit information

The following information resides in the United States, regardless of the region hosting your Cloud Insights environment:

- Environment site (sometimes called "tenant") information such as site/account owner.
- Information that allows NetApp Cloud Central to communicate with regional Cloud Insights sites, including anything to do with user Authorization.
- Information related to the relation between the Cloud Insights user and the tenant.

Host Regions

Host regions include:

- US: us-east-1
- EMEA: eu-central-1

- APAC: ap-southeast-2

More Information

You can read more about NetApp's privacy and security at the following links:

- [Trust Center](#)
- [Cross-Border Data Transfers](#)
- [Binding Corporate Rules](#)
- [Responding to Third-Party Data Requests](#)
- [NetApp Privacy Principles](#)

Getting Started

Feature Tutorials

Cloud Insights is loaded with useful features that enable you to quickly and easily find data, troubleshoot issues, and provide insights into your corporate environment. Find data easily with powerful queries, visualize data in dashboards, and send email alerts for data thresholds you set.

Cloud Insights includes a number of video tutorials to help you understand these features and better implement your business insight strategies. Every user who has access to your Cloud Insights environment can take advantage of these tutorials.

Introduction

Watch a brief tutorial explaining how Cloud Insights works.

► <https://docs.netapp.com/us-en/cloudinsights//media/howTo.mp4> (video)

Checklist and Video Tutorials

The **Startup Checklist** displayed on your Cloud Insights site contains a list of several useful tasks and concepts. Selecting an item in the checklist takes you to the appropriate Cloud Insights page for that concept. For example, clicking on the *Create a Dashboard* item opens the Cloud Insights **Dashboards** page.



At the top of the page is a link to a video tutorial showing how to create a dashboard. You can view the video as many times as you like until you click the *Got it! Don't Show This Again* link for that video. The video is available every time you go to the Dashboards page, until you dismiss it.



After watching the video at least once, the *Create a Dashboard* item in the checklist is checked off, indicating that you have completed the tutorial. You can then proceed to the next tutorial.



You can view the tutorials in any order you like, as many times as you like until dismissed.

Dismissing the Checklist

The Startup Checklist is displayed on your site until you click the *Don't Show This Again* link at the bottom of the checklist. Even after dismissing the checklist, the tutorials are still available on each appropriate Cloud Insights page until you dismiss each one from the message header bar.

View the Tutorials

Querying Data

- ▶ <https://docs.netapp.com/us-en/cloudinsights//media/Queries.mp4> (video)

Creating a Dashboard

- ▶ <https://docs.netapp.com/us-en/cloudinsights//media/Dashboards.mp4> (video)

Troubleshooting

- ▶ <https://docs.netapp.com/us-en/cloudinsights//media/Troubleshooting.mp4> (video)

Resolve Devices

- ▶ https://docs.netapp.com/us-en/cloudinsights//media/AHR_small.mp4 (video)

Collecting Data

Getting started gathering data

After you have signed up for Cloud Insights and log in to your environment for the first time, you will be guided through the following steps in order to begin collecting and managing data.

Data collectors discover information from your data sources, such as storage devices, network switches, and virtual machines. The information gathered is used for analysis, validation, monitoring and troubleshooting.

Cloud Insights has available three types of data collectors:

- Infrastructure (storage devices, network switches, compute infrastructure)
- Operating Systems (such as VMWare or Windows)
- Services (such as Kafka)

Select your first data collector from the supported vendors and models available. You can easily add additional data collectors later.

Install an Acquisition Unit

If you selected an *Infrastructure* data collector, an Acquisition Unit is required to inject data into Cloud Insights. You will need to download and install the Acquisition Unit software on a server or VM on the data center from which you will be collecting. A single Acquisition Unit can be used for multiple data collectors.

Install Acquisition Unit

Cloud Insights collects device data via one or more Acquisition Units installed on local servers. Each Acquisition Unit can host multiple Data Collectors, which send device metrics to Cloud Insights for analysis.

What Operating System or Platform Are You Using?

Linux



Linux Versions Supported

Production Best Practices

[Need Help?](#)

Installation Instructions

1 Copy Installer Snippet

This snippet has a unique key valid for 24 hours for this Acquisition Unit only.

Reveal Installer Snippet

2 Paste the snippet into a bash shell to run the installer.

3 Waiting for Acquisition Unit to connect...

- Follow the [Instructions](#) displayed to install your Acquisition Unit. Once the Acquisition Unit software is installed, the Continue button is displayed and you can proceed to the next step.

3 Continue New acquisition unit detected!

You may set up additional acquisition units later if needed. For example, you may want different Acquisition Units collecting information from data centers in different regions.

Configure the Data Collector - Infrastructure

For *Infrastructure* data collectors, you will be asked to fill out the data collector fields presented:

- Give the data collector a unique and meaningful name.
- Enter the credentials (user name and password) to connect to the device, as appropriate.
- Fill in any other mandatory fields in *Configuration* and *Advanced Configuration* sections.
- Click **Add Collector** to save the data collector.

You will be able to configure additional data collectors later.

Configure the Data Collector - Operating Systems and Services

Operating System:

For *Operating System* data collectors, choose a platform (MacOS, Linux, Windows) to install a Cloud Insights Agent.

You must have at least one agent to collect data from Services.

The agent also collects data from the host itself, for use in Cloud Insights. This data is categorized as "Node" data in widgets, etc.

- Open a terminal or command window on the agent host or VM, and paste the displayed command to install

the agent.

- When installation is complete, click **Complete Setup**.

Services:

For Service data collectors, click on a tile to open the instructions page for that service.

- Choose a platform and an Agent Access Key.
- If you don't have an agent installed on that platform, follow the instructions to install the agent.
- Click **Continue** to open the data collector instruction page.
- Follow the instructions to configure the data collector.
- When configuration is complete, click **Complete Setup**.

Add Dashboards

Depending on the type of initial data collector you selected to configure (storage, switch, etc.), one or more relevant dashboards will be imported. For example, if you configured a storage data collector, a set of storage-related dashboards will be imported, and one will be set as your Cloud Insights Home Page. You can change the home page from the **Dashboards > Show All Dashboards** list.

You can import additional dashboards later, or [create your own](#).

That's all there is to it

After you complete the initial setup process, your environment will begin to collect data.

If your initial setup process is interrupted (for example, if you close the browser window), you will need to follow the steps manually:

- Choose a Data Collector
- Install an Agent or Acquisition Unit if prompted
- Configure the Data Collector

Useful definitions

The following definitions may be useful when talking about Cloud Insights data collectors or features:

- Collector life cycle: A collector will belong to one of the following states in its life cycle:
 - **Preview:** Available in a limited capacity or to a limited audience. [Preview features](#) and data collectors are expected to become GA following the preview period. Preview periods vary based on audience or functionality.
 - **GA:** A feature or data collector that is Generally Available to all customers, based on Edition or feature set.
 - **Deprecated:** Applies to data collectors that are, or are expected to become, no longer functionally sustainable. Deprecated data collectors are often replaced with newer, functionally-updated data collectors.
 - **Deleted:** A data collector that has been removed and is no longer available.
- Acquisition Unit: a computer dedicated to hosting data collectors, typically a Virtual Machine. This computer is typically located in the same data center / VPC as the monitored items.

- Data Source: a module for communicating with a hardware or software stack. It consists of a configuration and code that runs on the AU computer to communicate with the device.

Acquisition Unit Requirements

You must install an Acquisition Unit (AU) in order to acquire information from your infrastructure data collectors (storage, VM, port, EC2, etc.). Before you install the Acquisition Unit, you should ensure that your environment meets operating system, CPU, memory, and disk space requirements.

Requirements

Component	Linux Requirement	Windows Requirement
Operating system	<p>A computer running a licensed version of one of the following:</p> <ul style="list-style-type: none"> * Centos (64-bit): 7.2 through 7.9, Stream 8, Stream 9 * Debian (64-bit): 9 and 10 * Oracle Enterprise Linux (64-bit): 7.5 through 7.9, 8.1 through 8.4 * Red Hat Enterprise Linux (64-bit): 7.2 through 7.9, 8.1 through 8.6 * Ubuntu Server: 18.04 and 20.04 LTS <p>This computer should be running no other application-level software. A dedicated server is recommended.</p>	<p>A computer running a licensed version of one of the following:</p> <ul style="list-style-type: none"> * Microsoft Windows 10 64-bit * Microsoft Windows Server 2012 * Microsoft Windows Server 2012 R2 * Microsoft Windows Server 2016 * Microsoft Windows Server 2019 * Microsoft Windows Server 2022 * Microsoft Windows 11 <p>This computer should be running no other application-level software. A dedicated server is recommended.</p>
CPU	2 CPU cores	Same
Memory	8 GB RAM	Same
Available disk space	<p>50 GB</p> <p>For Linux, disk space should be allocated in this manner:</p> <ul style="list-style-type: none"> /opt/netapp 10 GB /var/log/netapp 40 GB /tmp at least 1 GB available during installation 	50 GB

Network	<p>100 Mbps/1 Gbps Ethernet connection, static IP address, and port 80 or 443 connectivity from Acquisition Unit to *.cloudinsights.netapp.com or your Cloud Insights environment (i.e. https://<environment_id>.c01.cloudinsights.netapp.com) is required.</p> <p>For requirements between Acquisition Unit and each Data Collector, please refer to instructions for the Data Collector.</p> <p>If your organization requires proxy usage for internet access, you may need to understand your organization's proxy behavior and seek certain exceptions for Cloud Insights to work. For example, does your organization block access by default, and only allow access to specific web sites/domains by exception? If so, you will need to get the following domain added to the exception list:</p> <p>*.cloudinsights.netapp.com</p> <p>For more information, ready about Proxies here or here.</p>	Same
Permissions	Sudo permissions on the Acquisition Unit server. /tmp must be mounted with exec capabilities.	Administrator permissions on the Acquisition Unit server
Virus Scan		During installation, you must completely disable all virus scanners. Following installation, the paths used by the Acquisition Unit software must be excluded from virus scanning.

Additional recommendations

- For accurate audit and data reporting, it is strongly recommended to synchronize the time on the Acquisition Unit machine using **Network Time Protocol (NTP)** or **Simple Network Time Protocol (SNTP)**.

Regarding Sizing

You can get started with a Cloud Insights Acquisition Unit with just 8GB memory and 50GB of disk space, however, for larger environments you should ask yourself the following questions:

Do you expect to:

- Discover more than 2500 virtual machines or 10 large (> 2 node) ONTAP clusters, Symmetrix, or HDS/HPE VSP/XP arrays on this Acquisition Unit?
- Deploy 75 or more total data collectors on this Acquisition Unit?

For each "Yes" answer above, it is recommended to add 8 GB of memory and 50 GB of disk space to the AU. So for example if you answered "Yes" to both, you should deploy a 24GB memory system with 150GB or more of disk space. On Linux, the disk space to be added to the log location.

For additional sizing questions, contact NetApp Support.

Configuring Acquisition Units

Cloud Insights collects device data using one or more Acquisition Units installed on local servers. Each Acquisition Unit can host multiple Data Collectors, which send device metrics to Cloud Insights for analysis.

This topic describes how to add Acquisition Units and describes additional steps required when your environment uses a proxy.



For accurate audit and data reporting, it is strongly recommended to synchronize the time on the Acquisition Unit machine using **Network Time Protocol (NTP)** or **Simple Network Time Protocol (SNTP)**.

Adding a Linux Acquisition Unit

Before you begin

- If your system is using a proxy, you must set the proxy environment variables before the acquisition unit is installed. For more information, see [Setting proxy environment variables](#).

Steps for Linux Acquisition Unit Installation

1. Log in as Administrator or Account Owner to your Cloud Insights environment.
2. Click **Admin > Data Collectors > Acquisition Units > +Acquisition Unit**

The system displays the *Install Acquisition Unit* dialog. Choose Linux.

Install Acquisition Unit

Cloud Insights collects device data via one or more Acquisition Units installed on local servers. Each Acquisition Unit can host multiple Data Collectors, which send device metrics to Cloud Insights for analysis.

What Operating System or Platform Are You Using?



Linux



Linux Versions Supported

Production Best Practices

[Need Help?](#)

Installation Instructions

1[Copy Installer Snippet](#)

This snippet has a unique key valid for 24 hours for this Acquisition Unit only.

[Reveal Installer Snippet](#)**2**

Paste the snippet into a bash shell to run the installer.

3

Waiting for Acquisition Unit to connect...

1. Verify that the server or VM hosting the Acquisition Unit meets the recommended system requirements.
2. Verify that the server is running a supported version of Linux. Click *OS Versions Supported (i)* for a list of supported versions.
3. Copy the Installation command snippet in the dialog into a terminal window on the server or VM that will host the Acquisition unit.
4. Paste and execute the command in the Bash shell.

After you finish

- Click **Admin > Data Collectors > Acquisition units** to check the status of Acquisition Units.
- You can access the Acquisition Unit logs at /var/log/netapp/cloudinsights/acq/acq.log
- Use the following script to control the Acquisition Unit:
 - cloudinsights-service.sh (stop, start, restart, check the status)
- Use the following script to uninstall the Acquisition Unit:
 - cloudinsights-uninstall.sh

Setting proxy environment variables

For environments that use a proxy, you must set the proxy environment variables before you add the Acquisition Unit. The instructions for configuring the proxy are provided on the *Add Acquisition Unit* dialog.

1. Click + in *Have a Proxy Server?*
2. Copy the commands to a text editor and set your proxy variables as needed.

Note: Be aware of restrictions on special characters in proxy username and password fields: '%' and '!' are allowed in the username field. '.', '%', and '!' are allowed in the password field.

3. Run the edited command in a terminal using the Bash shell.
4. Install the Acquisition Unit software.

Proxy Configuration

The Acquisition Unit uses 2-way/mutual authentication to connect to the Cloud Insights server. The client certificate must be passed to the Cloud Insights server to be authenticated. To accomplish this, the proxy must be set up to forward the https request to the Cloud Insights server without decrypting the data.

The simplest way to do this is to specify wildcard configuration in your proxy/firewall to communicate with Cloud Insights, for example:

```
*.cloudinsights.netapp.com
```



The use of an asterisk (*) for wildcard is common, but your proxy/firewall configuration may use a different format. Check with your proxy documentation to ensure correct wildcard specification in your environment.

More information on proxy configuration can be found in the NetApp [Knowledgbase](#).

Viewing Proxy URLs

You can view your proxy endpoint URLs by clicking the **Proxy Settings** link when choosing a data collector during onboarding, or the link under *Proxy Settings* on the **Help > Support** page. A table like the following is displayed.

Proxy Settings					X
If your organization requires proxy usage for internet access, you need to understand your organization's proxy behavior and seek certain exceptions for Cloud Insights to work. The simplest way is to add the following domains to the exception list:					Close
Hostname	Port	Protocol	Methods	Endpoint URL Purpose	
qtrjkso.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Tenant	
00b1100.1234.abcd.12bc.a1b2c3ef56a7.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Ingestion	
aulogin.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Authentication	
portal.proxy.cloud.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Gateway	

If you have Workload Security in your environment, the configured endpoint URLs will also be displayed in this list.

Adding a Windows Acquisition Unit

Steps for Windows Acquisition Unit Installation

1. Log in to the Acquisition Unit server/VM as a user with Administrator permissions.
2. On that server, open a browser window and log in to your Cloud Insights environment as Administrator or Account Owner.
3. Click **Admin > Data Collectors > Acquisition Units > +Acquisition Unit**.

The system displays the *Install Acquisition Unit* dialog. Choose Windows.

Install Acquisition Unit

Cloud Insights collects device data via one or more Acquisition Units installed on local servers. Each Acquisition Unit can host multiple Data Collectors, which send device metrics to Cloud Insights for analysis.

What Operating System or Platform Are You Using?

Windows ▼ Windows Versions Supported i Production Best Practices i

Installation Instructions

[Need Help?](#)

1 [Download Installer \(Windows 64-bit\)](#)

2 [Copy Access Key](#)

This access key is a unique key valid for 24 hours for this Acquisition Unit only.

[Reveal Access Key](#)

3 Paste access key into installer when prompted.

4 Please ensure you have copied and pasted the access key into the installer.

[Have a Proxy Server?](#)

- 1 Verify that the server or VM hosting the Acquisition Unit meets the recommended system requirements.
- 2 Verify that the server is running a supported version of Windows. Click *OS Versions Supported (i)* for a list of supported versions.
- 3 Click the **Download Installer (Windows 64-bit)** button.
- 4 Copy the Access Key. You will need this during the Installation.
- 5 On the Acquisition Unit server/VM, execute the downloaded installer.
- 6 Paste the Access Key into the installation wizard when prompted.
- 7 During installation, you will be presented with the opportunity to provide your proxy server settings.

After you finish

- Click **Admin > Data Collectors > Acquisition units** to check the status of Acquisition Units.
- You can access the Acquisition Unit log in <install dir>\Cloud Insights\Acquisition Unit\log\acq.log
- Use the following script to stop, start, restart, or check the status of the Acquisition Unit:

```
cloudinsights-service.sh
```

Proxy Configuration

The Acquisition Unit uses 2-way/mutual authentication to connect to the Cloud Insights server. The client certificate must be passed to the Cloud Insights server to be authenticated. To accomplish this, the proxy must be set up to forward the https request to the Cloud Insights server without decrypting the data.

The simplest way to do this is to specify wildcard configuration in your proxy/firewall to communicate with Cloud Insights, for example:

*.cloudinsights.netapp.com



The use of an asterisk (*) for wildcard is common, but your proxy/firewall configuration may use a different format. Check with your proxy documentation to ensure correct wildcard specification in your environment.

More information on proxy configuration can be found in the NetApp [Knowledgbase](#).

Viewing Proxy URLs

You can view your proxy endpoint URLs by clicking the **Proxy Settings** link when choosing a data collector during onboarding, or the link under *Proxy Settings* on the **Help > Support** page. A table like the following is displayed.

Proxy Settings					X
If your organization requires proxy usage for internet access, you need to understand your organization's proxy behavior and seek certain exceptions for Cloud Insights to work. The simplest way is to add the following domains to the exception list:					
Hostname	Port	Protocol	Methods	Endpoint URL Purpose	
qtrjkso.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Tenant	
00b1100.1234.abcd.12bc.a1b2c3ef56a7.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Ingestion	
aulogin.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Authentication	
portal.proxy.cloud.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Gateway	

[Close](#)

If you have Workload Security in your environment, the configured endpoint URLs will also be displayed in this list.

Uninstalling an Acquisition Unit

To uninstall the Acquisition Unit software, do the following:

Windows:

If you are uninstalling a **Windows** acquisition unit:

1. On the Acquisition Unit server/VM, open Control Panel and choose **Uninstall a Program**. Select the Cloud Insights Acquisition Unit program for removal.
2. Click Uninstall and follow the prompts.

Linux:

If you are uninstalling a **Linux** acquisition unit:

1. On the Acquisition Unit server/VM, run the following command:

```
sudo cloudinsights-uninstall.sh -p
```

2. For help with uninstall, run:

```
sudo cloudinsights-uninstall.sh --help
```

Windows and Linux:

After uninstalling the AU:

1. In Cloud Insights, go to **Admin > Data Collectors** and select the **Acquisition Units** tab.
2. Click the Options button to the right of the Acquisition Unit you wish to uninstall, and select *Delete*. You can delete an Acquisition Unit only if there are no data collectors assigned to it.

NOTE: You cannot delete the default Acquisition Unit. Select another AU as the default before deleting the old one.

Reinstalling an Acquisition Unit

To re-install an Acquisition Unit on the same server/VM, you must follow these steps:

Before you begin

You must have a temporary Acquisition Unit configured on a separate server/VM before re-installing an Acquisition Unit.

Steps

1. Log in to the Acquisition Unit server/VM and uninstall the AU software.
2. Log into your Cloud Insights environment and go to **Admin > Data Collectors**.
3. For each data collector, click the Options menu on the right and select *Edit*. Assign the data collector to the temporary Acquisition Unit and click **Save**.

You can also select multiple data collectors of the same type and click the **Bulk Actions** button. Choose *Edit* and assign the data collectors to the temporary Acquisition Unit.

4. After all of the data collectors have been moved to the temporary Acquisition Unit, go to **Admin > Data Collectors** and select the **Acquisition Units** tab.
5. Click the Options button to the right of the Acquisition Unit you wish to re-install, and select *Delete*. You can delete an Acquisition Unit only if there are no data collectors assigned to it.
6. You can now re-install the Acquisition Unit software on the original server/VM. Click **+Acquisition Unit** and follow the instructions above to install the Acquisition Unit.
7. Once the Acquisition Unit has been re-installed, assign your data collectors back to the Acquisition Unit.

Viewing AU Details

The Acquisition Unit (AU) detail page provides useful detail for an AU as well as information to help with troubleshooting. The AU detail page contains the following sections:

- A **summary** section showing the following:
 - **Name** and **IP** of the Acquisition Unit
 - Current connection **Status** of the AU
 - **Last Reported** successful data collector poll time
 - The **Operating System** of the AU machine
 - Any current **Note** for the AU. Use this field to enter a comment for the AU. The field displays the most recently added note.
- A table of the AU's **Data Collectors** showing, for each data collector:
 - **Name** - Click this link to drill down into the data collector's detail page with additional information
 - **Status** - Success or error information
 - **Type** - Vendor/model
 - **IP** address of the data collector
 - Current **Impact** level
 - **Last Acquired** time - when the data collector was last successfully polled

Acquisition Unit Summary					
Name xp-linux	Connection Status OK- Need Help?	Operating System Linux	Note		
IP 10.197.120.145	Last Reported 2 minutes ago				
<hr/>					
Data Collectors (3)					
<input type="checkbox"/> Name ↑	Status	Type	IP	Impact	Last Acquired
foo	! Inventory failed	NetApp Data ONTAP 7-Mode	foo	Low	Never
xp-cisco	All successful	Cisco MDS Fabric Switches	10.197.136.66		2 minutes ago
<input type="checkbox"/> xpcdot26	All successful	NetApp ONTAP Data Management Software	10.197.136.26		8 minutes ago

For each data collector, you can click on the "three dots" menu to Clone, Edit, Poll, or Delete the data collector. You can also select multiple data collectors in this list to perform bulk actions on them.

To restart the Acquisition Unit, click the **Restart** button at the top of the page. Drop down this button to attempt to **Restore Connection** to the AU in the event of a connection problem.

Configuring an Agent to Collect Data (Windows/Linux/Mac)

Cloud Insights uses **Telegraf** as its agent for collection of integration data. Telegraf is a plugin-driven server agent that can be used to collect and report metrics, events, and logs. Input plugins are used to collect the desired information into the agent by accessing

the system/OS directly, by calling third-party APIs, or by listening to configured streams (i.e. Kafka, statsD, etc). Output plugins are used to send the collected metrics, events, and logs from the agent to Cloud Insights.

The current Telegraf version for Cloud Insights is **1.24.0**.



For accurate audit and data reporting, it is strongly recommended to synchronize the time on the Agent machine using **Network Time Protocol (NTP)** or **Simple Network Time Protocol (SNTP)**.



If you want to verify the installation files before installing the Agent, see the section below on [Verifying Checksums](#).

Installing an Agent

If you are installing a Service data collector and have not yet configured an Agent, you are prompted to first install an Agent for the appropriate Operating System. This topic provides instructions for installing the Telegraf agent on the following Operating Systems:

- [Windows](#)
- [RHEL and CentOS](#)
- [Ubuntu and Debian](#)
- [macOS](#)
- [Kubernetes](#)

To install an agent, regardless of the platform you are using, you must first do the following:

1. Log into the host you will use for your agent.
 2. Log in to your Cloud Insights site and go to **Admin > Data Collectors**.
 3. Click on **+Data Collector** and choose a data collector to install.
1. Choose the appropriate platform for your host (Windows, Linux, macOS, etc.)
 2. Follow the remaining steps for each platform.



Once you have installed an agent on a host, you do not need to install an agent again on that host.



Once you have installed an agent on a server/VM, Cloud Insights collects metrics from that system in addition to collecting from any data collectors you configure. These metrics are gathered as "[Node](#)" metrics.



If you are using a proxy, read the proxy instructions for your platform before installing the Telegraf agent.

Windows

Pre-requisites:

- PowerShell must be installed
- If you are behind a proxy, you must follow the instructions in the **Configuring Proxy Support for Windows** section.

Configuring Proxy Support for Windows



If your environment uses a proxy, read this section before you install.



The steps below outline the actions needed to set the *http_proxy/https_proxy* environment variables. For some proxy environments, users may also need to set the *no_proxy* environment variable.

For systems residing behind a proxy, perform the following to set the *https_proxy* and/or *http_proxy* environment variable(s) **PRIOR** to installing the Telegraf agent:

```
[System.Environment]::SetEnvironmentVariable("https_proxy",
    "<proxy_server>:<proxy_port>",
    [System.EnvironmentVariableTarget]::Machine)
```

Installing the agent



Install Agent

Quickly setup an agent in your environment and immediately start monitoring data

Select existing API Access Token or create a new one

KEY1 (...Zqlk0c)

+ API Access Token

Need Help?

1

[Copy Agent Installer Snippet](#)

This snippet has a unique key and is valid for 24 hours. Already have an agent in your environment? [View Troubleshooting](#)

[Reveal Agent Installer Snippet](#)

2

Open a PowerShell window as administrator and paste the snippet

3

[Complete Setup](#)

Steps to install agent on Windows:

1. Choose an Agent Access Key.
2. Copy the command block from the agent installation dialog. You can click the clipboard icon to quickly copy the command to the clipboard.
3. Open a PowerShell window

4. Paste the command into the PowerShell window and press Enter.
5. The command will download the appropriate agent installer, install it, and set a default configuration. When finished, it will restart the agent service. The command has a unique key and is valid for 24 hours.
6. Click **Finish** or **Continue**

After the agent is installed, you can use the following commands to start/stop the service:

```
Start-Service telegraf  
Stop-Service telegraf
```

Uninstalling the Agent

To uninstall the agent on Windows, do the following in a PowerShell window:

1. Stop and delete the Telegraf service:

```
Stop-Service telegraf  
sc.exe delete telegraf
```

2. Remove the certificate from the trustore:

```
cd Cert:\CurrentUser\Root  
//rm E5FB7B68C08B1CA902708584C274F8EFC7BE8ABC  
rm 1A918038E8E127BB5C87A202DF173B97A05B4996
```

3. Delete the `C:\Program Files\telegraf` folder to remove the binary, logs, and configuration files
4. Remove the `SYSTEM\CurrentControlSet\Services\EventLog\Application\telegraf` key from the registry

Upgrading the Agent

To upgrade the telegraf agent, do the following:

1. Stop and delete the telegraf service:

```
Stop-Service telegraf  
sc.exe delete telegraf
```

2. Delete the `SYSTEM\CurrentControlSet\Services\EventLog\Application\telegraf` key from the registry
3. Delete `C:\Program Files\telegraf\telegraf.conf`
4. Delete `C:\Program Files\telegraf\telegraf.exe`
5. [Install the new agent](#).

RHEL and CentOS

Pre-requisites:

- The following commands must be available: curl, sudo, ping, sha256sum, openssl, and dmidecode
- If you are behind a proxy, you must follow the instructions in the [Configuring Proxy Support for RHEL/CentOS](#) section.

Configuring Proxy Support for RHEL/CentOS



If your environment uses a proxy, read this section before you install.



The steps below outline the actions needed to set the *http_proxy/https_proxy* environment variables. For some proxy environments, users may also need to set the *no_proxy environment* variable.

For systems residing behind a proxy, perform the following steps **PRIOR** to installing the Telegraf agent:

1. Set the *https_proxy* and/or *http_proxy* environment variable(s) for the current user:

```
export https_proxy=<proxy_server>:<proxy_port>
```

2. Create */etc/default/telegraf*, and insert definitions for the *https_proxy* and/or *http_proxy* variable(s):

```
https_proxy=<proxy_server>:<proxy_port>
```

Installing the agent



Install Agent

Quickly setup an agent in your environment and immediately start monitoring data

Select existing API Access Token or create a new one

default_ingestion_api_key1 (...xEKVyK)

+ API Access Token

Production Best Practices ?

Installation Instructions

Need Help?

- 1 For environments operating behind a proxy server, follow the instructions to [configure proxy support to install and run Telegraf](#).

- 2 [Copy Agent Installer Snippet](#)

This snippet has a unique key and is valid for 24 hours. Already have an agent in your environment? [View Troubleshooting](#)

Reveal Agent Installer Snippet

- 3 Open a terminal window and paste the snippet in a Bash shell (requires curl, sudo, ping, sha256sum, and dmidecode).

- 4 [Complete Setup](#)

Steps to install agent on RHEL/CentOS:

1. Choose an Agent Access Key.
2. Copy the command block from the agent installation dialog. You can click the clipboard icon to quickly copy the command to the clipboard.
3. Open a Bash window
4. Paste the command into the Bash window and press Enter.
5. The command will download the appropriate agent installer, install it, and set a default configuration. When finished, it will restart the agent service. The command has a unique key and is valid for 24 hours.
6. Click **Finish** or **Continue**

After the agent is installed, you can use the following commands to start/stop the service:

If your operating system is using systemd (CentOS 7+ and RHEL 7+):

```
sudo systemctl start telegraf
sudo systemctl stop telegraf
```

If your operating system is not using systemd (CentOS 7+ and RHEL 7+):

```
sudo service telegraf start
sudo service telegraf stop
```

Uninstalling the Agent

To uninstall the agent on RHEL/CentOS, in a Bash terminal, do the following:

1. Stop the Telegraf service:

```
systemctl stop telegraf (If your operating system is using systemd  
(CentOS 7+ and RHEL 7+)  
/etc/init.d/telegraf stop (for systems without systemd support)
```

2. Remove the Telegraf agent:

```
yum remove telegraf
```

3. Remove any configuration or log files that may be left behind:

```
rm -rf /etc/telegraf*  
rm -rf /var/log/telegraf*
```

Upgrading the Agent

To upgrade the telegraf agent, do the following:

1. Stop the telegraf service:

```
systemctl stop telegraf (If your operating system is using systemd  
(CentOS 7+ and RHEL 7+)  
/etc/init.d/telegraf stop (for systems without systemd support)
```

2. Remove the previous telegraf agent:

```
yum remove telegraf
```

3. [Install the new agent.](#)

Ubuntu and Debian

Pre-requisites:

- The following commands must be available: curl, sudo, ping, sha256sum, openssl, and dmidecode
- If you are behind a proxy, you must follow the instructions in the [Configuring Proxy Support for Ubuntu/Debian](#) section.

Configuring Proxy Support for Ubuntu/Debian



If your environment uses a proxy, read this section before you install.



The steps below outline the actions needed to set the `http_proxy/https_proxy` environment variables. For some proxy environments, users may also need to set the `no_proxy` environment variable.

For systems residing behind a proxy, perform the following steps **PRIOR** to installing the Telegraf agent:

1. Set the `https_proxy` and/or `http_proxy` environment variable(s) for the current user:

```
export https_proxy=<proxy_server>:<proxy_port>
```

2. Create `/etc/default/telegraf`, and insert definitions for the `https_proxy` and/or `http_proxy` variable(s):

```
https_proxy=<proxy_server>:<proxy_port>
```

Installing the agent



Ubuntu & Debian

Install Agent

Quickly setup an agent in your environment and immediately start monitoring data

Select existing API Access Token or create a new one

default_ingestion_api_key1 (...xEKVyK)

+ API Access Token

Production Best Practices

Installation Instructions

Need Help?

- 1 For environments operating behind a proxy server, follow the instructions to [configure proxy support to install and run Telegraf](#).

- 2 [Copy Agent Installer Snippet](#)

This snippet has a unique key and is valid for 24 hours. Already have an agent in your environment? [View Troubleshooting](#)

[Reveal Agent Installer Snippet](#)

- 3 Open a terminal window and paste the snippet in a Bash shell (requires curl, sudo, ping, sha256sum, and dmidecode).

- 4 [Complete Setup](#)

Steps to install agent on Debian or Ubuntu:

1. Choose an Agent Access Key.
2. Copy the command block from the agent installation dialog. You can click the clipboard icon to quickly copy the command to the clipboard.

3. Open a Bash window
4. Paste the command into the Bash window and press Enter.
5. The command will download the appropriate agent installer, install it, and set a default configuration. When finished, it will restart the agent service. The command has a unique key and is valid for 24 hours.
6. Click **Finish or Continue**

After the agent is installed, you can use the following commands to start/stop the service:

If your operating system is using systemd:

```
sudo systemctl start telegraf  
sudo systemctl stop telegraf
```

If your operating system is not using systemd:

```
sudo service telegraf start  
sudo service telegraf stop
```

Uninstalling the Agent

To uninstall the agent on Ubuntu/Debian, in a Bash terminal, run the following:

1. Stop the Telegraf service:

```
systemctl stop telegraf (If your operating system is using systemd)  
/etc/init.d/telegraf stop (for systems without systemd support)
```

2. Remove the Telegraf agent:

```
dpkg -r telegraf
```

3. Remove any configuration or log files that may be left behind:

```
rm -rf /etc/telegraf*  
rm -rf /var/log/telegraf*
```

Upgrading the Agent

To upgrade the telegraf agent, do the following:

1. Stop the telegraf service:

```
systemctl stop telegraf (If your operating system is using systemd)  
/etc/init.d/telegraf stop (for systems without systemd support)
```

2. Remove the previous telegraf agent:

```
dpkg -r telegraf
```

3. [Install the new agent.](#)

macOS

Pre-requisites:

- The following commands must be available: curl, sudo, openssl, and shasum
- If you are behind a proxy, you must follow the instructions in the [Configuring Proxy Support for macOS](#) section.

Configuring Proxy Support for macOS



If your environment uses a proxy, read this section before you install.



The steps below outline the actions needed to set the *http_proxy/https_proxy* environment variables. For some proxy environments, users may also need to set the *no_proxy environment* variable.

For systems residing behind a proxy, perform the following to set the *https_proxy* and/or *http_proxy* environment variable(s) for the current user **PRIOR** to installing the Telegraf agent:

```
export https_proxy=<proxy_server>:<proxy_port>
```

AFTER installing the Telegraf agent, add and set the appropriate *https_proxy* and/or *http_proxy* variable(s) in */Applications/telegraf.app/Contents/telegraf.plist*:

```

...
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>EnvironmentVariables</key>
    <dict>
        <key>https_proxy</key>
        <string><proxy_server>:<proxy_port></string>
    </dict>
    <key>Program</key>
    <string>/Applications/telegraf.app/Contents/MacOS/telegraf</string>
    <key>Label</key>
    <string>telegraf</string>
    <key>ProgramArguments</key>
    <array>
        <string>/Applications/telegraf.app/Contents/MacOS/telegraf</string>
        <string>--config</string>
        <string>/usr/local/etc/telegraf.conf</string>
        <string>--config-directory</string>
        <string>/usr/local/etc/telegraf.d</string>
    </array>
    <key>RunAtLoad</key>
    <true/>
</dict>
</plist>
...

```

Then, restart Telegraf after loading the above changes:

```

sudo launchctl stop telegraf
sudo launchctl unload -w /Library/LaunchDaemons/telegraf.plist
sudo launchctl load -w /Library/LaunchDaemons/telegraf.plist
sudo launchctl start telegraf

```

Installing the agent



Install Agent

Quickly setup an agent in your environment and immediately start monitoring data

Select existing API Access Token or create a new one

default_ingestion_api_key1 (...xEKVyK)

+ API Access Token

Production Best Practices

Need Help?

Installation Instructions

- 1 For environments operating behind a proxy server, follow the instructions to [configure proxy support to install and run Telegraf](#).

- 2 [Copy Agent Installer Snippet](#)

This snippet has a unique key and is valid for 24 hours. Already have an agent in your environment? [View Troubleshooting](#)

[Reveal Agent Installer Snippet](#)

- 3 Open a terminal window and paste the snippet in a Bash shell (requires sudo, shasum, and curl).

- 4 [Complete Setup](#)

Steps to install agent on macOS:

1. Choose an Agent Access Key.
2. Copy the command block from the agent installation dialog. You can click the clipboard icon to quickly copy the command to the clipboard.
3. Open a Bash window
4. Paste the command into the Bash window and press Enter.
5. The command will download the appropriate agent installer, install it, and set a default configuration. When finished, it will restart the agent service. The command has a unique key and is valid for 24 hours.
6. If you previously installed a Telegraf agent using Homebrew, you will be prompted to uninstall it. Once the previously installed Telegraf agent is uninstalled, re-run the command in step 5 above.
7. Click **Finish** or **Continue**

After the agent is installed, you can use the following commands to start/stop the service:

```
sudo launchctl start telegraf
sudo launchctl stop telegraf
```

Uninstalling the Agent

To uninstall the agent on macOS, in a Bash terminal, run the following:

1. Stop the Telegraf service:

```
sudo launchctl stop telegraf
```

2. Uninstall the telegraf agent:

```
sudo cp /Applications/telegraf.app/scripts/uninstall /tmp  
sudo /tmp/uninstall
```

3. Remove any configuration or log files that may be left behind:

```
sudo rm -rf /usr/local/etc/telegraf*  
sudo rm -rf /usr/local/var/log/telegraf.*
```

Upgrading the Agent

To upgrade the telegraf agent, do the following:

1. Stop the telegraf service:

```
sudo launchctl stop telegraf
```

2. Uninstall the previous telegraf agent:

```
sudo cp /Applications/telegraf.app/scripts/uninstall /tmp  
sudo /tmp/uninstall
```

3. [Install the new agent.](#)

Kubernetes

The NetApp Kubernetes Monitoring Operator (NKMO) is the preferred method for installing Kubernetes for Cloud Insights Insights, for more flexible configuration of monitoring in fewer steps, as well as enhanced opportunities for monitoring other software running in the K8s cluster.

Please [go here](#) for information and installation instructions for the NetApp Kubernetes Monitoring Operator.

Verifying Checksums

The Cloud Insights agent installer performs integrity checks, but some users may want to perform their own verifications before installing or applying downloaded artifacts. This can be done by downloading the installer and generating a checksum for the downloaded package, then comparing the checksum to the value shown in the install instructions.

Download the installer package without installing

To perform a download-only operation (as opposed to the default download-and-install), users can edit the agent installation command obtained from the UI and remove the trailing “install” option.

Follow these steps:

1. Copy the Agent Installer snippet as directed.
2. Instead of pasting the snippet into a command window, paste it into a text editor.
3. Remove the trailing “--install” (Linux/Mac) or “-install” (Windows) from the command.
4. Copy the entire command from the text editor.
5. Now paste it into your command window (in a working directory) and run it.

Non-Windows (these examples are for Kubernetes; actual script names may vary):

- Download and install (default):

```
installerName=cloudinsights-kubernetes.sh ... && sudo -E -H  
./$installerName --download --install
```

- Download-only:

```
installerName=cloudinsights-kubernetes.sh ... && sudo -E -H  
./$installerName --download
```

Windows:

- Download and install (default):

```
!$(installerName=".\\cloudinsights-windows.ps1") ... -and  
$(installerName -download -install)
```

- Download-only:

```
!$(installerName=".\\cloudinsights-windows.ps1") ... -and  
$(installerName -download)
```

The download-only command will download all required artifacts from Cloud Insights to the working directory.

The artifacts include, but may not be limited to:

- an installation script
- an environment file
- YAML files
- a signed checksum file (ending in sha256.signed or sha256.ps1)
- a PEM file (netapp_cert.pem) for signature verification

The installation script, environment file, and YAML files can be verified using visual inspection.

The PEM file can be verified by confirming its fingerprint to be the following:

```
1A918038E8E127BB5C87A202DF173B97A05B4996
```

More specifically,

- Non-Windows:

```
openssl x509 -fingerprint -sha1 -noout -inform pem -in netapp_cert.pem
```

- Windows:

```
Import-Certificate -Filepath .\netapp_cert.pem -CertStoreLocation Cert:\CurrentUser\Root
```

Generate checksum value

To generate the checksum value, perform the following command for your appropriate platform:

- RHEL/Ubuntu:

```
sha256sum <package_name>
```

- macOS:

```
shasum -a 256 telegraf.pkg
```

- Windows:

```
Get-FileHash telegraf.zip -Algorithm SHA256 | Format-List
```

Verify checksum using PEM file

The signed checksum file can be verified using the PEM file:

- Non-Windows:

```
openssl smime -verify -in telegraf*.sha256.signed -CAfile netapp_cert.pem  
-purpose any
```

- Windows (after installing the certificate via Import-Certificate above):

```
Get-AuthenticodeSignature -FilePath .\telegraf.zip.sha256.ps1  
$result = Get-AuthenticodeSignature -FilePath .\telegraf.zip.sha256.ps1  
$signer = $result.SignerCertificate  
Add-Type -Assembly System.Security  
[Security.Cryptography.X509Certificates.X509Certificate2UI]::DisplayCertificate($signer)
```

Install the downloaded package

Once all of the artifacts have been satisfactorily verified, the agent installation can be initiated by running:

Non-Windows:

```
sudo -E -H ./<installation_script_name> --install
```

Windows:

```
.\cloudinsights-windows.ps1 -install
```

Troubleshooting

Some things to try if you encounter problems setting up an agent:

Problem:	Try this:
After configuring a new plugin and restarting Telegraf, Telegraf fails to start up. The logs indicate that an error resembling the following: "[telegraf] Error running agent: Error loading config file /etc/telegraf/telegraf.d/cloudinsights-default.conf: plugin outputs.http: line <linenumber>: configuration specified the fields ["use_system_proxy"], but they weren't used"	The installed Telegraf version is outdated. Follow the steps on this page to Upgrade the Agent for your appropriate platform.

Problem:	Try this:
I ran the installer script on an old installation and now the agent isn't sending data	Uninstall the telegraf agent and then re-run the installation script. Follow the Upgrade the Agent steps on this page for your appropriate platform.
I already installed an agent using Cloud Insights	If you have already installed an agent on your host/VM, you do not need to install the agent again. In this case, simply choose the appropriate Platform and Key in the Agent Installation screen, and click on Continue or Finish .
I already have an agent installed but not by using the Cloud Insights installer	Remove the previous agent and run the Cloud Insights Agent installation, to ensure proper default configuration file settings. When complete, click on Continue or Finish .

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Configuring the NetApp Kubernetes Monitoring Operator

Cloud Insights uses a number of components, including [Fluent Bit](#) and [Telegraf](#), for collection of Kubernetes data. Telegraf is a plugin-driven server agent that can be used to collect and report metrics, events, and logs. Input plugins are used to collect the desired information into the agent by accessing the system/OS directly, by calling third-party APIs, or by listening to configured streams (i.e. Kafka, statsD, etc). Output plugins are used to send the collected metrics, events, and logs from the agent to Cloud Insights.

Cloud Insights offers the **NetApp Kubernetes Monitoring Operator** (NKMO) for Kubernetes collection. When adding a data collector, simply choose the "Kubernetes" tile.

Choose a Data Collector to Monitor



Below is a high-level illustration showing where the Operator resides in your environment. Depending on your environment, *Proxy Server* may or may not be required.

The Operator (NKMO) and the data collectors are downloaded from the Cloud Insights Docker Registry. Once installed, NKMO then manages any Operator-compatible collectors deployed in the Kubernetes cluster nodes to acquire data, including managing the life cycle of those collectors. Following this chain, data is acquired from the collectors and sent through to Cloud Insights.

Before installing the NetApp Kubernetes Monitoring Operator

Pre-requisites:

- Please note the following component versions. These are the current *required* versions included with the NetApp Kubernetes Monitoring Operator. You will particularly need to note these versions if you are [using a custom or private docker repository](#):
 - Telegraf: 1.25.0
 - kube-rbac-proxy: v0.13.0
 - kube-state-metrics: v2.6.0
 - fluent-bit: 1.9.8
 - kubernetes-event-exporter: v0.10
- NetApp Kubernetes Monitoring Operator installation is supported with Kubernetes version 1.20 or greater.
- When Cloud Insights is monitoring the backend storage and Kubernetes is used with the Docker container runtime, Cloud Insights can display pod-to-PV-to-storage mappings and metrics for NFS and iSCSI; other runtimes only show NFS.
- Beginning August 2022, the NetApp Kubernetes Monitoring Operator includes support for Pod Security Policy (PSP). You must [upgrade](#) to the latest NetApp Kubernetes Monitoring Operator if your environment uses PSP.
- If you are running on OpenShift 4.6 or higher, you must follow the **OpenShift Instructions** below in addition to ensuring these pre-requisites are met.
- Monitoring is only installed on Linux nodes

Cloud Insights supports monitoring of Kubernetes nodes that are running Linux, by specifying a Kubernetes node selector that looks for the following Kubernetes labels on these platforms:

Platform	Label
Kubernetes v1.20 and above	Kubernetes.io/os = linux
Rancher + cattle.io as orchestration/Kubernetes platform	cattle.io/os = linux

- The NetApp Kubernetes Monitoring Operator and its dependencies (telegraf, kube-state-metrics, fluentbit, etc.) are not supported on nodes that are running with Arm64 architecture.
- The following commands must be available: *curl*, *sudo*, *openssl*, *sha256sum*, and *kubectl*. For best results, add these commands to the PATH. Note that *kubectl* needs to be configured with access to the following kubernetes objects at a minimum: *agents*, *clusterroles*, *clusterrolebindings*, *customresourcedefinitions*, *deployments*, *namespaces*, *roles*, *rolebindings*, *secrets*, *serviceaccounts*, and *services*. See [here](#) for an example .yaml file with these minimum clusterrole privileges.
- The host you will use for the NetApp Kubernetes Monitoring Operator installation must have *kubectl* configured to communicate with the target K8s cluster, and have Internet connectivity to your Cloud Insights environment. If this host requires a proxy to reach Cloud Insights, follow the instructions in the [Configuring Proxy Support](#) section.
- The NetApp Kubernetes Monitoring Operator installs its own kube-state-metrics to avoid conflict with any other instances.
- If you are behind a proxy during installation, or when operating the K8s cluster to be monitored, follow the instructions in the [Configuring Proxy Support](#) section.
- You must have permissions to create Kubernetes cluster roles and role bindings.

For accurate audit and data reporting, it is strongly recommended to synchronize the time on the Agent machine using **Network Time Protocol (NTP)** or **Simple Network Time Protocol (SNTP)**.

Note these before you start

If you are running with a [proxy](#), have a [custom repository](#), or are using [OpenShift](#), read the following sections carefully.

If you are upgrading from a previous installation, also read the [Upgrading](#) information.

If you want to verify the installation files before installing the Agent, read about [Verifying Kubernetes Checksums](#).

Configuring Proxy Support

There are two places where you may use a proxy in your environment in order to install the NetApp Kubernetes Monitoring Operator. These may be the same or separate proxy systems:

- Proxy needed during execution of the installation code snippet (using "curl") to connect the system where the snippet is executed to your Cloud Insights environment
- Proxy needed by the target Kubernetes cluster to communicate with your Cloud Insights environment

If you use a proxy for either or both of these, in order to install the NetApp Kubernetes Operating Monitor you must first ensure that your proxy is configured to allow good communication to your Cloud Insights environment. If you have a proxy and can access Cloud Insights from the server/VM from which you wish to install the Operator, then your proxy is likely configured properly.

For the proxy used to install the NetApp Kubernetes Operating Monitor, before installing the Operator, set the `http_proxy/https_proxy` environment variables. For some proxy environments, you may also need to set the `no_proxy` environment variable.

To set the variable(s), perform the following steps on your system **before** installing the NetApp Kubernetes Monitoring Operator:

1. Set the `https_proxy` and/or `http_proxy` environment variable(s) for the current user:

- a. If the proxy being setup does not have Authentication (username/password), run the following command:

```
export https_proxy=<proxy_server>:<proxy_port>
```

- b. If the proxy being setup does have Authentication (username/password), run this command:

```
export http_proxy=
<proxy_username>:<proxy_password>@<proxy_server>:<proxy_port>
```

For the proxy used for your Kubernetes cluster to communicate with your Cloud Insights environment, install the NetApp Kubernetes Monitoring Operator after reading all of these instructions.

To finish the configuration, perform the following steps on the system **after** you have installed the NetApp Kubernetes Monitoring Operator.

First, open the `agent-monitoring-netapp` file for editing:

```
kubectl -n netapp-monitoring edit agent agent-monitoring-netapp
```

Locate the **spec:** section of this file and add the following code:

```
proxy:

# If an AU is enabled on your cluster for monitoring
# by Cloud Insights, then isAuProxyEnabled should be set to true:
isAuProxyEnabled: <true or false>

# If your Operator install is behind a corporate proxy,
# isTelegrafProxyEnabled should be set to true:
isTelegrafProxyEnabled: <true or false>

# If LOGS_COLLECTION is enabled on your cluster for monitoring
# by CI, then isFluentbitProxyEnabled should be set to true:
isFluentbitProxyEnabled: <true or false>

# Set the following values according to your proxy login:
password: <password for proxy, optional>
port: <port for proxy>
server: <server for proxy>
username: <username for proxy, optional>

# In the noProxy section, enter a comma-separated list of
# IP addresses and/or resolvable hostnames that should bypass
# the proxy:
noProxy: <comma separated list>
```

Using a custom or private docker repository

By default, the NetApp Kubernetes Monitoring Operator config will pull container images from public registries. If you have a Kubernetes cluster used as the target for monitoring, and that cluster is configured to only pull container images from a custom or private Docker repository or container registry, you must configure access to the containers needed by the NetApp Kubernetes Monitoring Operator so the necessary commands can be executed.

Use the following instructions to pre-position container images in your registry and alter the NetApp Kubernetes Monitoring Operator config to access those images. Substitute your chosen installation namespace in the following commands if it differs from the default namespace of “netapp-monitoring”.

1. Get the docker secret:

```
kubectl -n netapp-monitoring get secret docker -o yaml
```

2. Copy/paste the value of `.dockerconfigjson`: from the output of the above command.

3. Decode the docker secret:

```
echo <paste from _.dockerconfigjson:_ output above> | base64 -d
```

The output of this will be in the following JSON format:

```
{ "auths":  
  { "docker.<cluster>.cloudinsights.netapp.com" :  
    {"username":"<tenant id>",  
     "password":"<password which is the CI API token>",  
     "auth"      :"<encoded username:password basic auth token. This is  
internal to docker>"}  
  }  
}
```

Log in to the docker repository:

```
docker login docker.<cluster>.cloudinsights.netapp.com (from step #2) -u  
<username from step #2>  
password: <password from docker secret step above>
```

Pull the operator docker image from Cloud Insights. Make sure the *netapp-monitoring* version number is current:

```
docker pull docker.<cluster>.cloudinsights.netapp.com/netapp-  
monitoring:<version>  
docker pull docker.<cluster>.cloudinsights.netapp.com/distroless-root-  
user:<version>
```

Find the *netapp-monitoring* <version> field using the following command:

```
kubectl -n netapp-monitoring describe deployment monitoring-operator |  
grep -i "image:" |grep netapp-monitoring
```

Download all open source dependencies to your private docker registry. The following open source images need to be downloaded. See the [Pre-requisites](#) section above for the most current versions of these components:

```
docker pull docker.<cluster>.cloudinsights.netapp.com/telegraf:<telegraf version>
docker pull docker.<cluster>.cloudinsights.netapp.com/kube-rbac-proxy:<kube-rbac-proxy version>
docker pull docker.<cluster>.cloudinsights.netapp.com/kube-state-metrics:<kube-state-metrics version>
```

If fluent-bit is enabled, also download:

```
docker pull docker.<cluster>.cloudinsights.netapp.com/fluent-bit:<fluent-bit version>
docker pull docker.<cluster>.cloudinsights.netapp.com/kubernetes-event-exporter:<kubernetes-event-exporter version>
```

Push the operator docker image to your private/local/enterprise docker repository according to your corporate policies. Ensure that the directory paths to these images in your repository are consistent with that in docker.<cluster>.cloudinsights.netapp.com.

Edit the monitoring-operator deployment, and modify all image references to use the new docker repo location:

```
image: <docker repo of the enterprise/corp docker repo>/kube-rbac-proxy:<kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-monitoring:<version>
```

Edit the agent CR to reflect the new docker repo location.

```
kubectl -n netapp-monitoring edit agent agent-monitoring-netapp
```

```
docker-repo: <docker repo of the enterprise/corp docker repo>
dockerRepoSecret: <optional: name of the docker secret of enterprise/corp docker repo, this secret should be already created on the k8s cluster in the same namespace>
```

In the *spec:* section, make the following changes:

```
spec:  
  telegraf:  
    - name: ksm  
      substitutions:  
        - key: k8s.gcr.io  
          value: <same as "docker-repo" field above>
```

OpenShift Instructions

If you are running on OpenShift 4.6 or higher, you must change the "privileged-mode" setting. Run the following command to open the agent for editing. If you are using a namespace other than "netapp-monitoring", specify that namespace in the command line:

```
kubectl edit agent agent-monitoring-netapp -n netapp-monitoring
```

In the file, change *privileged-mode: false* to *privileged-mode: true*

Openshift may implement an added level of security that may block access to some Kubernetes components.

Installing the NetApp Kubernetes Monitoring Operator

Deploy NetApp Monitoring Operator

Quickly install and configure a Kubernetes Operator to send cluster information to Cloud Insights.

Select existing API Access Token or create a new one

default_new_k8s_operator_api_key1 (...PHBwgZ)

+ API Access Token

Production Best Practices ?

Installation Instructions

[Need Help?](#)

- Supply a name for kubernetes cluster and identify a namespace to be used, or created, for the installation of monitoring components. Once entered, the code of installation snippet is generated and becomes available for download. Monitoring is only installed on Linux nodes

Cluster

ClusterName

Namespace

netapp-monitoring

2

[Copy Agent Installer Snippet](#)

This snippet has a unique key and is valid for 24 hours. Already have an agent in your environment? [View Troubleshooting](#)

[+ Reveal Agent Installer Snippet](#)

3

Successful execution of code snippet relies on presence of *curl* and *kubectl*.

- The default configuration for *kubectl* should point to the kubernetes cluster to be monitored.
- To execute the code snippet from a system where a proxy is required to access the CI tenant, [follow instructions here](#).

Paste the supplied code snippet and execute it at a *bash* prompt.

- For environments operating behind a proxy server, follow the [instructions to configure proxy support for the installed agent](#)
- For Kubernetes clusters configured to access container images from a custom/private container registry, follow the [instructions to configure a custom/private repository for the installed agent](#).

4

[Next](#)

Steps to install NetApp Kubernetes Monitoring Operator agent on Kubernetes:

- Enter a unique cluster name and namespace. If you are [upgrading](#) from the script-based agent or a previous Kubernetes Operator, use the same cluster name and namespace.
- Once these are entered, you can copy the Agent Installer snippet
- Click the button to copy this snippet to the clipboard.
- Paste the snippet into a *bash* window and execute it. Note that the snippet has a unique key and is valid for 24 hours.
- The installation proceeds automatically. When it is complete, click the *Complete Setup* button.



Setup is incomplete until you [configure your proxy](#).



If you have a custom repository, you must follow the instructions for [Using a custom/private docker repository](#).

Upgrading



If you have a previously installed script-based agent, you *must* upgrade to the NetApp Kubernetes Monitoring Operator.

Upgrading from script-based agent to NetApp Kubernetes Monitoring Operator

To upgrade the telegraf agent, do the following:

1. Make note of your cluster name as recognized by Cloud Insights. You can view the cluster name by running the following command. If your namespace is not the default (*ci-monitoring*), substitute the appropriate namespace:

```
kubectl -n ci-monitoring get cm telegraf-conf -o jsonpath='{.data}' | grep "kubernetes_cluster ="
```

1. Save the K8s cluster name for use during installation of the K8s operator-based monitoring solution to ensure data continuity.

If you do not remember the name of the K8s cluster in CI, it can be extracted from your saved configuration with the following command line:

```
cat /tmp/telegraf-configs.yaml | grep kubernetes_cluster | head -2
```

2. Remove the script-based monitoring

To uninstall the script-based agent on Kubernetes, do the following:

If the monitoring namespace is being used solely for Telegraf:

```
kubectl --namespace ci-monitoring delete ds,rs,cm,sa,clusterrole,clusterrolebinding -l app=ci-telegraf
```

```
kubectl delete ns ci-monitoring
```

If the monitoring namespace is being used for other purposes in addition to Telegraf:

```
kubectl --namespace ci-monitoring delete ds,rs,cm,sa,clusterrole,clusterrolebinding -l app=ci-telegraf
```

3. [Install](#) the current Operator. Be sure to use the same cluster name noted in step 1 above.

Upgrading to the latest NetApp Kubernetes Monitoring Operator

For Operator-based installation upgrades, run the following commands:

- Make note of your cluster name as recognized by Cloud Insights. You can view the cluster name by running the following command. If your namespace is not the default (*netapp-monitoring*), substitute the appropriate namespace:

```
kubectl -n netapp-monitoring get agent -o jsonpath='{.items[0].spec.cluster-name}'
```

[Uninstall](#) the current Operator.

[Install](#) the latest Operator. Use the same cluster name, and ensure you are pulling new container images if you have set up a custom repo.

Stopping and Starting the Netapp Kubernetes Monitoring Operator

To stop the Netapp Kubernetes Monitoring Operator:

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=0
```

To start the Netapp Kubernetes Monitoring Operator:

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=1
```

Uninstalling



If you are running on a previously-installed script-based Kubernetes agent, you must [upgrade](#) to the NetApp Kubernetes Monitoring Operator.

To remove the deprecated script-based agent

Note that these commands are using the default namespace "ci-monitoring". If you have set your own namespace, substitute that namespace in these and all subsequent commands and files.

To uninstall the script-based agent on Kubernetes (for example, when upgrading to the NetApp Kubernetes Monitoring Operator), do the following:

If the monitoring namespace is being used solely for Telegraf:

```
kubectl --namespace ci-monitoring delete ds,rs,cm,sa,clusterrole,clusterrolebinding -l app=ci-telegraf
```

```
kubectl delete ns ci-monitoring
```

If the monitoring namespace is being used for other purposes in addition to Telegraf:

```
kubectl --namespace ci-monitoring delete ds,rs,cm,sa,clusterrole,clusterrolebinding -l app=ci-telegraf
```

To remove the NetApp Kubernetes Monitoring Operator

Note that the default namespace for the NetApp Kubernetes Monitoring Operator is "netapp-monitoring". If you have set your own namespace, substitute that namespace in these and all subsequent commands and files.

Newer versions of the monitoring operator can be uninstalled with the following commands:

```
kubectl delete agent -A -l installed-by=nkmo-<name-space>
kubectl delete ns,clusterrole,clusterrolebinding,crd -l installed-by=nkmo-
<name-space>
```

If the first command returns "No resources found", use the following instructions to uninstall older versions of the monitoring operator.

Execute each of the following commands in order. Depending on your current installation, some of these commands may return 'object not found' messages. These messages may be safely ignored.

```
kubectl -n <NAMESPACE> delete agent agent-monitoring-netapp
kubectl delete crd agents.monitoring.netapp.com
kubectl -n <NAMESPACE> delete role agent-leader-election-role
kubectl delete clusterrole agent-manager-role agent-proxy-role agent-
metrics-reader <NAMESPACE>-agent-manager-role <NAMESPACE>-agent-proxy-role
<NAMESPACE>-cluster-role-privileged
kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-
rolebinding agent-cluster-admin-rolebinding <NAMESPACE>-agent-manager-
rolebinding <NAMESPACE>-agent-proxy-rolebinding <NAMESPACE>-cluster-role-
binding-privileged
kubectl delete <NAMESPACE>-psp-nkmo
kubectl delete ns <NAMESPACE>
```

If a Security Context Constraint was previously-created manually for a script-based Telegraf installation:

```
kubectl delete scc telegraf-hostaccess
```

About Kube-state-metrics

The NetApp Kubernetes Monitoring Operator installs kube-state-metrics automatically; no user interaction is needed.

kube-state-metrics Counters

Use the following links to access information for these kube state metrics counters:

1. [ConfigMap Metrics](#)
2. [DaemonSet Metrics](#)
3. [Deployment Metrics](#)

4. [Ingress Metrics](#)
5. [Namespace Metrics](#)
6. [Node Metrics](#)
7. [Persistent Volume Metrics](#)
8. [Persistent Volume Claim Metrics](#)
9. [Pod Metrics](#)
10. [ReplicaSet metrics](#)
11. [Secret metrics](#)
12. [Service metrics](#)
13. [StatefulSet metrics](#)

Verifying Kubernetes Checksums

The Cloud Insights agent installer performs integrity checks, but some users may want to perform their own verifications before installing or applying downloaded artifacts. To perform a download-only operation (as opposed to the default download-and-install), these users can edit the agent installation command obtained from the UI and remove the trailing “install” option.

Follow these steps:

1. Copy the Agent Installer snippet as directed.
2. Instead of pasting the snippet into a command window, paste it into a text editor.
3. Remove the trailing “--install” from the command.
4. Copy the entire command from the text editor.
5. Now paste it into your command window (in a working directory) and run it.
 - Download and install (default):

```
installerName=cloudinsights-kubernetes.sh ... && sudo -E -H  
./$installerName --download --install
```

- Download-only:

```
installerName=cloudinsights-kubernetes.sh ... && sudo -E -H  
./$installerName --download
```

The download-only command will download all required artifacts from Cloud Insights to the working directory. The artifacts include, but may not be limited to:

- an installation script
- an environment file
- YAML files
- a signed checksum file (sha256.signed)

- a PEM file (netapp_cert.pem) for signature verification

The installation script, environment file, and YAML files can be verified using visual inspection.

The PEM file can be verified by confirming its fingerprint to be the following:

```
1A918038E8E127BB5C87A202DF173B97A05B4996
```

More specifically,

```
openssl x509 -fingerprint -sha1 -noout -inform pem -in netapp_cert.pem
```

The signed checksum file can be verified using the PEM file:

```
openssl smime -verify -in sha256.signed -CAfile netapp_cert.pem -purpose any
```

Once all of the artifacts have been satisfactorily verified, the agent installation can be initiated by running:

```
sudo -E -H ./<installation_script_name> --install
```

Tuning the Operator

You can adjust the NetApp Kubernetes Monitoring Operator for optimal performance by fine-tuning certain variables for Custom Resources. For instructions and lists of the variables you can tune, see the README file included with the installation package. After you have installed the operator, use the following command to view the README:

```
kubectl exec -c manager -it <operator-pod-name> -n <namespace> -- cat configs/substitution-vars/README.txt
```

Troubleshooting

Some things to try if you encounter problems setting up the NetApp Kubernetes Monitoring Operator:

Problem:	Try this:
I do not see a hyperlink/connection between my Kubernetes Persistent Volume and the corresponding back-end storage device. My Kubernetes Persistent Volume is configured using the hostname of the storage server.	Follow the steps to uninstall the existing Telegraf agent, then re-install the latest Telegraf agent. You must be using Telegraf version 2.0 or later, and your Kubernetes cluster storage must be actively monitored by Cloud Insights.

Problem:	Try this:
<p>I'm seeing messages in the logs resembling the following:</p> <pre>E0901 15:21:39.962145 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: Failed to list *v1.MutatingWebhookConfiguration: the server could not find the requested resource E0901 15:21:43.168161 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: Failed to list *v1.Lease: the server could not find the requested resource (get leases.coordination.k8s.io) etc.</pre>	<p>These messages may occur if you are running kube-state-metrics version 2.0.0 or above with Kubernetes versions below 1.20.</p> <p>To get the Kubernetes version:</p> <pre>kubectl version</pre> <p>To get the kube-state-metrics version:</p> <pre>kubectl get deploy/kube-state-metrics -o jsonpath='{..image}'</pre> <p>To prevent these messages from happening, users can modify their kube-state-metrics deployment to disable the following Leases:</p> <pre>mutatingwebhookconfigurations validatingwebhookconfigurations volumeattachments resources</pre> <p>More specifically, they can use the following CLI argument:</p> <pre>resources=certificatesigningrequests,configmaps,cron jobs,daemonsets, deployments,endpoints,horizontalpodautoscalers,ingr esses,jobs,limitranges, namespaces,networkpolicies,nodes,persistentvolume claims,persistentvolumes, poddisruptionbudgets,pods,replicasets,replicationcont rollers,resourcequotas, secrets,services,statefulsets,storageclasses</pre> <p>The default resource list is:</p> <pre>"certificatesigningrequests,configmaps,cronjobs,daem onsets,deployments, endpoints,horizontalpodautoscalers,ingresses,jobs,lea ses,limitranges, mutatingwebhookconfigurations,namespaces,networ kpolicies,nodes, persistentvolumeclaims,persistentvolumes,poddisrupti onbudgets,pods,replicasets, replicationcontrollers,resourcequotas,secrets,servic es, statefulsets,storageclasses, validatingwebhookconfigurations,volumeattachments"</pre>

Problem:	Try this:
<p>I see error messages from Telegraf resembling the following, but Telegraf does start up and run:</p> <pre data-bbox="132 264 807 982">Oct 11 14:23:41 ip-172-31-39-47 systemd[1]: Started The plugin-driven server agent for reporting metrics into InfluxDB. Oct 11 14:23:41 ip-172-31-39-47 telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="failed to create cache directory. /etc/telegraf/.cache/snowflake, err: mkdir /etc/telegraf/.ca che: permission denied. ignored\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" Oct 11 14:23:41 ip-172-31-39-47 telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="failed to open. Ignored. open /etc/telegraf/.cache/snowflake/ocsp_response_cache.j son: no such file or directory\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" Oct 11 14:23:41 ip-172-31-39-47 telegraf[1827]: 2021- 10-11T14:23:41Z !! Starting Telegraf 1.19.3</pre>	<p>This is a known issue. Refer to This GitHub article for more details. As long as Telegraf is up and running, users can ignore these error messages.</p>
<p>On Kubernetes, my Telegraf pod(s) are reporting the following error:</p> <pre data-bbox="132 1087 807 1172">"Error in processing mountstats info: failed to open mountstats file: /hostfs/proc/1/mountstats, error: open /hostfs/proc/1/mountstats: permission denied"</pre>	<p>If SELinux is enabled and enforcing, it is likely preventing the Telegraf pod(s) from accessing the /proc/1/mountstats file on the Kubernetes nodes. To relax this restriction, edit the agent (<code>kubectl edit agent agent-monitoring-netapp</code>), and change "privileged-mode: false" to "privileged-mode: true"</p>
<p>On Kubernetes, my Telegraf ReplicaSet pod is reporting the following error:</p> <pre data-bbox="132 1341 807 1552">[inputs.prometheus] Error in plugin: could not load keypair /etc/kubernetes/pki/etcd/server.crt:/etc/kubernetes/pki/ etcd/server.key: open /etc/kubernetes/pki/etcd/server.crt: no such file or directory</pre>	<p>The Telegraf ReplicaSet pod is intended to run on a node designated as a master or for etcd. If the ReplicaSet pod is not running on one of these nodes, you will get these errors. Check to see if your master/etcd nodes have taints on them. If they do, add the necessary tolerations to the Telegraf ReplicaSet, <code>telegraf-rs</code>.</p> <p>For example, edit the ReplicaSet...</p> <pre data-bbox="824 1573 1142 1615">kubectl edit rs telegraf-rs</pre> <p>...and add the appropriate tolerations to the spec. Then, restart the ReplicaSet pod.</p>

Problem:	Try this:
I have a PSP/PSA environment. Does this affect my monitoring operator?	<p>If your Kubernetes cluster is running with Pod Security Policy (PSP) or Pod Security Admission (PSA) in place, you must upgrade to the latest NetApp Kubernetes Monitoring Operator. Follow these steps to upgrade to the current NKMO with support for PSP/PSA:</p> <ol style="list-style-type: none"> 1. Uninstall the previous monitoring operator: <pre>kubectl delete agent agent-monitoring-netapp -n netapp-monitoring kubectl delete ns netapp-monitoring kubectl delete crd agents.monitoring.netapp.com kubectl delete clusterrole agent-manager-role agent-proxy-role agent-metrics-reader kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-rolebinding agent-cluster-admin-rolebinding</pre> <ol style="list-style-type: none"> 2. Install the latest version of the monitoring operator.
I ran into issues trying to deploy the NKMO, and I have PSP/PSA in use.	<ol style="list-style-type: none"> 1. Edit the agent using the following command: <pre>kubectl -n <name-space> edit agent</pre> <ol style="list-style-type: none"> 2. Mark 'security-policy-enabled' as 'false'. This will disable Pod Security Policies and Pod Security Admission and allow the NKMO to deploy. Confirm by using the following commands: <pre>kubectl get psp (should show Pod Security Policy removed) kubectl get all -n <namespace> grep -i psp (should show that nothing is found)</pre>
'ImagePullBackoff' errors seen	<p>These errors may be seen if you have a custom or private docker repository and have not yet configured the NetApp Kubernetes Monitoring Operator to properly recognize it. Read more about configuring for custom/private repo.</p>

Problem:	Try this:
<p>I am having an issue with my monitoring-operator deployment, and the current documentation does not help me resolve it.</p>	<p>Capture or otherwise note the output from the following commands, and contact the Technical Support team.</p> <pre data-bbox="856 327 1460 728"> kubectl -n netapp-monitoring get all kubectl -n netapp-monitoring describe all kubectl -n netapp-monitoring logs <monitoring-operator-pod> --all -containers=true kubectl -n netapp-monitoring logs <telegraf-pod> --all -containers=true </pre>

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Configuring Data Collectors

You configure Data Collectors in your Cloud Insights environment to collect data from devices in the data center.

Before you begin

- You must have configured an Acquisition Unit before you can start collecting data.
- You need credentials for the devices from which you are collecting Data.
- Device network addresses, account information, and passwords are required for all devices you are collecting data from.

Steps

1. From the Cloud Insights menu, click **Admin > Data Collectors**

The system displays the available Data Collectors arranged by vendor.

2. Click **+ Collector** on the required vendor and select the data collector to configure.

In the dialog box you can configure the data collector and add an Acquisition Unit.

3. Enter a name for the data collector.

Names can contain letters (a-z), numbers (0-9), dashes (-), underscores (_), apostrophes ('), and periods (.).

4. Enter the Acquisition Unit to associate with this data collector.
5. Enter the required fields in the Configuration screen.
6. When prompted to configure notifications, choose to alert by Email, Webhook, or both, and choose the alert types on which to notify (Critical, Warning, Informational, and/or Resolved). You can choose to notify

to the Global Monitor Recipient list (configured in **Admin > Notifications**), or specify additional recipients. When ready to continue, click **Complete Setup**.

Customize notifications for this collector

ONTAP Default monitors are preconfigured to send email notifications to “**Global Monitor Recipient List**”, you can add additional email addresses for this data collector.

By Email Notify team on Send to
Critical, Warning, Informa... Global Monitor Recipient List
Other Email Recipients

By Webhook Enable webhook notification to add recipients

When viewing an **ONTAP data collector** landing page, you can modify the notifications by clicking the pencil icon in the "Notifications" field of the data collector summary section.



ONTAP Data Collector notifications take precedence over any specific Monitor notifications that are relevant to the cluster/data collector. The recipient list you set for the Data Collector itself will receive the data collector alerts. If there are no active data collector alerts, then monitor-generated alerts will be sent to specific monitor recipients.

Summary

Name testtomy	Notifications Global Monitor Recipient List	Type NetApp ONTAP Data Management Software	Inventory Recent Status Error. Message ID: 6D441563	Note
Acquisition Unit WIN2K19IMAGE installed by eugene		Types of Data Collected Inventory, Performance	Performance Recent Status Stand-by	

1. Click **Advanced Configuration** to add additional configuration fields. (Not all data collectors require advanced configuration.)
2. Click **Test Configuration** to verify that the data collector is properly configured.
3. Click **Add Collector** to save the configuration and add the data collector to your Cloud Insights tenant.

After adding a new data collector, Cloud Insights initiates three polls:

- 1st inventory poll: immediately
- 1st performance data poll to establish a baseline: immediately after inventory poll
- 2nd performance poll: within 15 seconds after completion of 1st performance poll

Polling then proceeds according to the configured inventory and performance poll intervals.

Determining data collector acquisition status

Because data collectors are the primary source of information for Cloud Insights, it is imperative that you ensure that they remain in a running state.

Data collector status is displayed in the upper right corner of any asset page as the message "Acquired N

"minutes ago", where N indicates the most recent acquisition time of the asset's data collector(s). The acquisition time/date is also displayed.

Clicking on the message displays a table with data collector name, status, and last successful acquisition time. If you are signed in as an Administrator, clicking on the data collector name link in the table takes you to detail page for that data collector.

Managing configured data collectors

The Installed Data Collectors page provides access to the data collectors that have been configured for Cloud Insights. You can use this page to modify existing data collectors.

Steps

1. In the Cloud Insights menu, click **Admin > Data Collectors**

The Available Data Collectors screen is displayed.

2. Click **Installed Data Collectors**

A list of all of the installed Data Collectors is displayed. The list provides collector name, status, the IP address the collector is accessing, and when data was last acquired from the a device. Action that can be performed on this screen include:

- Control polling
- Change data collector credentials
- Clone data collectors

Controlling Data Collector polling

After making a change to a data collector, you might want it to poll immediately to check your changes, or you might want to postpone the data collection on a data collector for one, three, or five days while you work on a problem.

Steps

1. In the Cloud Insights menu, click **Admin > Data Collectors**
2. Click **Installed Data Collectors**
3. Select the check box to the left of the Data Collector you want to change
4. Click **Bulk Actions** and select the polling action you want to take.

Bulk actions can be performed simultaneously on multiple Data Collectors. Select the data collectors, and chose the action to perform from the **Bulk Action** menu.

Editing data collector information

You can edit existing data collector setup information.

To edit a single data collector:

1. In the Cloud Insights menu, click **Admin > Data Collectors** to open the list of installed Data Collectors.
2. In the options menu to the right of the data collector you want to modify, click **Edit**.

The Edit Collector dialog is opened.

3. Enter the changes and click **Test Configuration** to test the new configuration or click **Save** to save the configuration.

You can also edit multiple data collectors:

1. Select the check box to the left of each data collector you want to change.
2. Click the **Bulk Actions** button and choose **Edit** to open the Edit data Collector dialog.
3. Modify the fields as above.



The data collectors selected must be the same vendor and model, and reside on the same Acquisition Unit.

When editing multiple data collectors, the Data Collector Name field shows “Mixed” and cannot be edited. Other fields such as user name and password show “Mixed” and can be edited. Fields that share the same value across the selected data collectors show the current values and can be edited.

When editing multiple data collectors, the **Test Configuration** button is not available.

Cloning data collectors

Using the clone facility, you can quickly add a data source that has the same credentials and attributes as another data source. Cloning allows you to easily configure multiple instances of the same device type.

Steps

1. In the Cloud Insights menu, click **Admin > Data Collectors**.
2. Click **Installed Data Collectors**.
3. Click the check box to the left of the data collector you want to copy.
4. In the options menu to the right of the selected data collector, click **Clone**.

The Clone Data Collector dialog is displayed.

5. Enter new information in the required fields.
6. Click **Save**.

After you finish

The clone operation copies all other attributes and settings to create the new data collector.

Performing bulk actions on data collectors

You can simultaneously edit some information for multiple data collectors. This feature allows you to initiate a poll, postpone polling, and resume polling on multiple data collectors. In addition, you can delete multiple data collectors.

Steps

1. In the Cloud Insights menu, click **Admin > Data Collectors**
2. Click **Installed Data Collectors**

3. Click the check box to the left of the data collectors you want to modify.
4. In the options menu to the right, click the option you want to perform.

After you finish

The operation you selected is performed on the data collectors. When you chose to delete data collectors, a dialog is displayed requiring you to confirm the action.

Researching a failed data collector

If a data collector has failure message and a High or Medium Impact, you need to research this problem using the data collector summary page with its linked information.

Use the following steps to determine the cause of failed data collectors. Data collector failure messages are displayed on the **Admin** menu and on the **Installed Data Collectors** page.

Steps

1. Click **Admin > Data Collectors > Installed Data Collectors**.
2. Click the linked Name of the failing data collector to open the Summary page.
3. On the Summary page, check the Comments area to read any notes that might have been left by another engineer who might also be investigating this failure.
4. Note any performance messages.
5. Move your mouse pointer over the segments of the Event Timeline graph to display additional information.
6. Select an error message for a Device and displayed below the Event Timeline and click the Error details icon that displays to the right of the message.

The Error details include the text of the error message, most likely causes, information in use, and suggestions of what can be tried to correct the problem.

7. In the Devices Reported By This Data Collector area, you might filter the list to display only devices of interest, and you can click the linked **Name** of a device to display the asset page for that device.
8. When you return to the data collector summary page, check the **Show Recent Changes** area at the bottom of the page to see if recent changes could have caused the problem.

Importing from the Dashboard Gallery

Cloud Insights provides a number of Recommended Dashboards to provide business insights into your data. Each dashboard contains widgets designed to help answer a particular question or solve a particular problem relevant to the data currently being collected in your environment.

To import a dashboard from the gallery, do the following:

1. Select **Dashboards > Dashboards**
2. Click on **+From Gallery**

A list of **Recommended Dashboards** is displayed. Each dashboard is named with a particular question the dashboard can help you solve. Dashboards are available to help answer questions around different types of objects, including AWS, NetApp, Storage, VMware, and others

3. Select one or more dashboards from the list and click **Add Dashboards**. These dashboards now show in your dashboard list.

In addition to the Recommended Dashboards, you can also choose to import **Additional Dashboards** that are not relevant to your current data. For example, if you have no storage data collectors currently installed but are planning on configuring some in the future, you may still choose to import the storage-relevant dashboards. These dashboards will be available for display but may not show any relevant data until at least one storage data collector is configured.

Importing from the dashboard gallery is available to users with Administrator or Account Owner role.

User Accounts and Roles

Cloud Insights provides up to four user account roles: Account Owner, Administrator, User, and Guest. Each account is assigned specific permission levels as noted in the table below. Users are either [invited](#) to Cloud Insights and assigned a specific role, or can sign in via [Single Sign-On \(SSO\) Authorization](#) with a default role. SSO Authorization is available as a feature in Cloud Insights Premium Edition.

Permission levels

You use an account that has Administrator privileges to create or modify user accounts. Each user account is assigned a role for each Cloud Insights feature from the following permission levels.

Role	Observability	Workload Security	Reporting
Account Owner	<p>Can modify subscriptions, view billing and usage information, and perform all Administrator functions for Observability, Security, and Reporting.</p> <p>Owners can also invite and manage users, as well as manage SSO Authentication and Identity Federation settings.</p> <p>The first Account Owner is created when you register for Cloud Insights.</p> <p>It is strongly recommended to have at least two Account Owners for each Cloud Insights environment.</p>		
Administrator	<p>Can perform all Observability functions, all user functions, as well as management of data collectors, Observability API tokens, and notifications.</p> <p>An Administrator can also invite other users but can only assign Observability roles.</p>	<p>Can perform all Security functions, including those for Alerts, Forensics, data collectors, automated response policies, and API tokens for Security.</p> <p>An Administrator can also invite other users but can only assign Security roles.</p>	<p>Can perform all User/Author functions including managing Reporting API tokens, as well as all administrative tasks such as configuration of reports, and the shutdown and restart of reporting tasks.</p> <p>An Administrator can also invite other users but can only assign Reporting roles.</p>

Role	Observability	Workload Security	Reporting
User	Can view and modify dashboards, queries, alerts, annotations, annotation rules, and applications, and manage device resolution.	Can view and manage Alerts and view Forensics. User role can change alert status, add a note, take snapshots manually, and manage restrict user access.	Can perform all Guest/Consumer functions as well as create and manage reports and dashboards.
Guest	Has read-only access to asset pages, dashboards, alerts, and can view and run queries.	Can view Alerts and Forensics. Guest role cannot change alert status, add a note, take snapshots manually, or restrict user access.	Can view, schedule, and run reports and set personal preferences such as those for languages and time zones. Guests/Consumers cannot create reports or perform administrative tasks.

Best practice is to limit the number of users with Administrator permissions. The greatest number of accounts should be user or guest accounts.

Cloud Insights Permissions by User Role

The following table shows the Cloud Insights permissions granted to each user role.

Feature	Administrator/ Account Owner	User	Guest
Acquisition Units: Add/Modify/Delete	Y	N	N
Alerts*: Create/Modify/Delete	Y	Y	N
Alerts*: View	Y	Y	Y
Annotation Rules: Create/Run/Modify/Delete	Y	Y	N
Annotations: Create/Modify/Assign/Vie w/Remove/Delete	Y	Y	N
API Access*: Create/Rename/Disable/R evoke	Y	N	N
Applications: Create/View/Modify/Delet e	Y	Y	N
Asset Pages: Modify	Y	Y	N
Asset Pages: View	Y	Y	Y
Audit: View	Y	N	N

Cloud Cost	Y	N	N
Security	Y	N	N
Dashboards: Create/Modify/Delete	Y	Y	N
Dashboards: View	Y	Y	Y
Data Collectors: Add/Modify/Poll/Delete	Y	N	N
Notifications: View/Modify	Y	N	N
Queries: Create/Modify/Delete	Y	Y	N
Queries: View/Run	Y	Y	Y
Device Resolution	Y	Y	N
Reports*: View/Run	Y	Y	Y
Reports*: Create/Modify/Delete/Schedule	Y	Y	N
Subscription: View/Modify	Y	N	N
User Management: Invite/Add/Modify/Deactivate	Y	N	N

*Requires Premium Edition

Creating Accounts by Inviting Users

Creating a new user account is achieved through Cloud Central. A user can respond to the invitation sent through email, but if the user does not have an account with Cloud Central, the user needs to sign up with Cloud Central so that they can accept the invitation.

Before you begin

- The user name is the email address of the invitation.
- Understand the user roles you will be assigning.
- Passwords are defined by the user during the sign up process.

Steps

- Log into Cloud Insights
- In the menu, click **Admin > User Management**

The User Management screen is displayed. The screen contains a list of all of the accounts on the system.

- Click **+ User**

The **Invite User** screen is displayed.

- Enter an email address or multiple addresses for invitations.

Note: When you enter multiple addresses, they are all created with the same role. You can only set multiple users to the same role.

1. Select the user's role for each feature of Cloud Insights.



The features and roles you can choose from depend on which features you have access to in your particular Administrator role. For example, if you have Admin role only for Reporting, you will be able to assign users to any role in Reporting, but will not be able to assign roles for Observability or Security.

Invite Users

You can invite people to join by sending them an invitation link. Inviting users is the easiest way to get your team to collaborate. Invitations expire after 14 days

X

Monitor & Optimize Role
Guest ▾

Cloud Secure Role
Administrator ▾

Cancel **Invite**

2. Click **Invite**

The invitation is sent to the user. Users will have 14 days to accept the invitation. Once a user accepts the invitation, they will be taken to the NetApp Cloud Portal, where they will sign up using the email address in the invitation. If they have an existing account for that email address, they can simply sign in and will then be able to access their Cloud Insights environment.

Modifying an existing user's role

To modify an existing user's role, including adding them as a **secondary account owner**, follow these steps.

1. Click **Admin > User Management**. The screen displays a list of all of the accounts on the system.
2. Click the user name of the account you want to change.
3. Modify the user's role in each Cloud Insights feature set as needed.

4. Click **Save Changes**.

To assign a Secondary Account Owner

You must be logged in as an account owner for Observability in order to assign the account owner role to another user.

1. Click **Admin > User Management**.
2. Click the user name of the account you want to change.
3. In the User dialog, click on **Assign as Owner**.
4. Save the changes.

The screenshot shows the user profile for 'Daniel'. At the top, it displays 'Daniel' and a close button ('X'). Below this, there's a table with two rows: 'Email' (user.name@netapp.com) and 'Last Login' (a year ago). A link 'Learn about the permissions provided by each role' is present. Under 'Owner Role', there's a button labeled 'Assign as Owner'. Below that, under 'Monitor & Optimize Role', there's a dropdown menu set to 'Administrator'. Under 'Cloud Secure Role', there's another dropdown menu also set to 'Administrator'. At the bottom right, there are three buttons: 'Delete User' (red), 'Cancel', and 'Save Changes'.

You can have as many account owners as you wish, but best practice is to limit the owner role to only select people.

Deleting Users

A user with the Administrator role can delete a user (for example, someone no longer with the company) by clicking on the user's name and clicking *Delete User* in the dialog. The user will be removed from the Cloud Insights environment.

Note that any dashboards, queries, etc. that were created by the user will remain available in the Cloud Insights environment even after the user is removed.

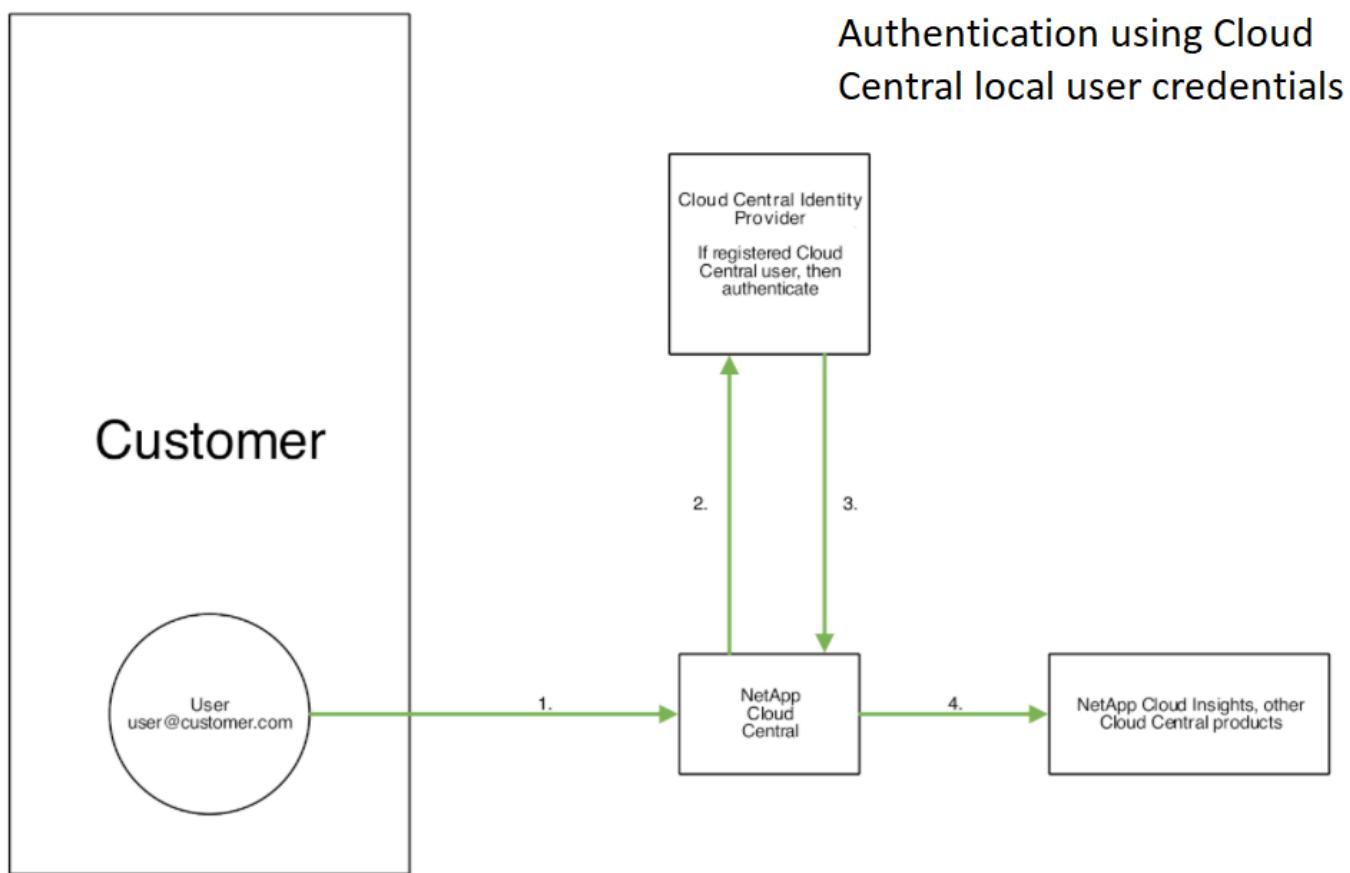
Single Sign-On (SSO) and Identity Federation

Enabling Identity Federation for SSO In Cloud Insights

With Identity Federation:

- Authentication is delegated to the customer's identity management system, using the customer's credentials from your corporate directory, and automation policies such as Multi-Factor Authentication (MFA).
- Users log in once to all NetApp Cloud Services (Single Sign On).

User accounts are managed in NetApp Cloud Central for all Cloud Services. By default, authentication is done using Cloud Central local user profile. Below is a simplified overview of that process:



However, some customers would like to use their own identity provider to authenticate their users for Cloud Insights and their other NetApp Cloud Central Services. With Identity Federation, NetApp Cloud Central accounts are authenticated using credentials from your corporate directory.

The following is a simplified example of that process:



In the above diagram, when a user accesses Cloud Insights, that user is directed to the customer's identity management system for authentication. Once the account is authenticated, the user is directed to the Cloud Insights tenant URL.

Cloud Central uses Auth0 to implement Identity Federation and integrate with services like Active Directory Federation Services (ADFS) and Microsoft Azure Active Directory (AD). For more information on Identity Federation setup and configuration, see Cloud Central documentation on [Identity Federation](#).

It is important to understand that changing identity federation in Cloud Central will apply not only to Cloud Insights but to all NetApp Cloud Services. The customer should discuss this change with the NetApp team of each Cloud Central product they own to make sure the configuration they are using will work with Identity Federation or if adjustments need to be made on any accounts. The customer will need to involve their internal SSO team in the change to identity federation as well.

It is also important to realize that once identity federation is enabled, that any changes to the company's identity provider (such moving from SAML to Microsoft AD) will likely require troubleshooting/changes/attention in Cloud Central to update the profiles of the users.

Single Sign-On (SSO) User Auto-Provisioning

In addition to inviting users, administrators can enable **Single Sign-On (SSO) User Auto-Provisioning** access to Cloud Insights for all users in their corporate domain, without having to invite them individually. With SSO enabled, any user with the same domain email address can log into Cloud Insights using their corporate credentials.



SSO User Auto-Provisioning is available in Cloud Insights Premium Edition, and must be configured before it can be enabled for Cloud Insights. SSO User Auto-Provisioning configuration includes [Identity Federation](#) through NetApp Cloud Central as described in the section above. Federation allows single sign-on users to access your NetApp Cloud Central accounts using credentials from your corporate directory, using open standards such as Security Assertion Markup Language 2.0 (SAML) and OpenID Connect (OIDC).

To configure *SSO User Auto-Provisioning*, on the **Admin > User Management** page, click the **Request Federation** button. Once configured, administrators can then enable SSO user login. When an administrator enables *SSO User Auto-Provisioning*, they choose a default role for all SSO users (such as Guest or User). Users who log in through SSO will have that default role.

The screenshot shows the 'User Management' page with a single user listed. The user has the name '(caitest12@netapp.com)', email 'caitest12@netapp.com', monitor role 'Administrator', reporting role 'Guest', and last login 'None'. There is a 'Request Federation' button at the top right.

Name	Email	Monitor & Optimize Role	Reporting Role	Last Login
(caitest12@netapp.com)	caitest12@netapp.com	Administrator	Guest	None

Occasionally, an administrator will want to promote a single user out of the default SSO role (for example, to make them an administrator). They can accomplish this on the **Admin > User Management** page by clicking on the right-side menu for the user and selecting *Assign Role*. Users who are assigned an explicit role in this way continue to have access to Cloud Insights even if *SSO User Auto-Provisioning* is subsequently disabled.

If the user no longer requires the elevated role, you can click the menu to *Remove User*. The user will be removed from the list. If *SSO User Auto-Provisioning* is enabled, the user can continue log in to Cloud Insights through SSO, with the default role.

You can choose to hide SSO users by unchecking the **Show SSO Users** checkbox.

However, do not enable *SSO User Auto-Provisioning* if either of these are true:

- Your organization has more than one Cloud Insights tenant
- Your organization does not want any/every user in the federated domain to have some level of automatic access to the Cloud Insights tenant. *At this point in time, we do not have the ability to use groups to control role access with this option.*

Cloud Insights Data Collector List

Cloud Insights supports a variety of Data Collectors from many vendors and services.

Data Collectors are categorized by these types:

- Infrastructure: Acquired from vendor devices such as storage arrays, switches, hypervisors, or backup devices.
- Service: Acquired from services such as Kubernetes or Docker. Also called *Integration*.

Alphabetical list of Data Collectors supported by Cloud Insights:

Data Collector	Type
ActiveMQ	Service
Amazon EC2 and EBS	Infrastructure
AWS S3 as Storage	Infrastructure
Amazon FSx for NetApp ONTAP	Infrastructure
Apache	Service
Azure NetApp Files	Infrastructure
Azure VMs and VHD	Infrastructure
Brocade Network Advisor (BNA)	Infrastructure
Brocade Fibre Channel Switches	Infrastructure
Cisco MDS Fabric Switches	Infrastructure
Consul	Service
Couchbase	Service
CouchDB	Service
Cohesity SmartFiles	Infrastructure
Dell EMC Data Domain	Infrastructure
Dell EMC ECS	Infrastructure
Dell EMC PowerScale (previously Isilon)	Infrastructure
Dell EMC Isilon / PowerScale REST	Infrastructure
Dell EMC PowerStore	Infrastructure
Dell EMC Recoverpoint	Infrastructure
Dell EMC ScaleIO	Infrastructure
Dell EMC Unity	Infrastructure
Dell EMC Unisphere REST	Infrastructure
Dell EMC VMAX/PowerMax Family of Devices	Infrastructure
Dell EMC VNX Block Storage	Infrastructure

Data Collector	Type
Dell EMC VNX File	Infrastructure
Dell EMC VNX Unified	Infrastructure
Dell EMC VPLEX	Infrastructure
Dell EMC XtremIO	Infrastructure
Dell XC Series	Infrastructure
Docker	Service
Elasticsearch	Service
Flink	Service
Fujitsu ETERNUS DX	Infrastructure
Google Compute and Storage	Infrastructure
Hadoop	Service
HAProxy	Service
Hitachi Content Platform (HCP)	Infrastructure
Hitachi Vantara Command Suite	Infrastructure
Hitachi Vantara NAS Platform	Infrastructure
Hitachi Ops Center	Infrastructure
HP Enterprise Alletra 6000 (previously Nimble) Storage	Infrastructure
HP Enterprise Alletra 9000 / Primera (previously 3PAR) Storage	Infrastructure
HP Enterprise Command View	Infrastructure
Huawei OceanStor and Dorado Devices	Infrastructure
IBM Cleversafe	Infrastructure
IBM CS Series	Infrastructure
IBM PowerVM	Infrastructure
IBM SAN Volume Controller (SVC)	Infrastructure
IBM System Storage DS8000 Series	Infrastructure
IBM XIV and A9000 Storages	Infrastructure
Infinidat InfiniBox	Infrastructure
Java	Service
Kafka	Service
Kapacitor	Service
Kibana	Service
Kubernetes	Service

Data Collector	Type
Lenovo HX Series	Infrastructure
macOS	Service
Memcached	Service
Microsoft Azure NetApp Files	Infrastructure
Microsoft Hyper-V	Infrastructure
MongoDB	Service
MySQL	Service
NetApp Cloud Volumes ONTAP	Infrastructure
NetApp Cloud Volumes Services for AWS	Infrastructure
NetApp Cloud Connection for ONTAP 9.9+	Infrastructure
NetApp Config Advisor	Infrastructure
NetApp Data ONTAP 7-Mode	Infrastructure
NetApp E-Series	Infrastructure
Amazon FSx for NetApp ONTAP	Infrastructure
NetApp HCI Virtual Center	Infrastructure
NetApp ONTAP Data Management Software	Infrastructure
NetApp ONTAP Select	Infrastructure
NetApp SolidFire All-Flash Array	Infrastructure
NetApp StorageGRID	Infrastructure
Netstat	Service
Nginx	Service
Node	Service
Nutanix NX Series	Infrastructure
OpenStack	Infrastructure
OpenZFS	Service
Oracle ZFS Storage Appliance	Infrastructure
PostgreSQL	Service
Puppet Agent	Service
Pure Storage FlashArray	Infrastructure
Red Hat Virtualization	Infrastructure
Redis	Service
RethinkDB	Service
RHEL & CentOS	Service

Data Collector	Type
Rubrik CDM Storage	Infrastructure
Ubuntu & Debian	Service
VMware vSphere	Infrastructure
Windows	Service
ZooKeeper	Service

Subscribing to Cloud Insights

Getting started with Cloud Insights is as easy as three simple steps:

- Sign up for an account on [NetApp Cloud Central](#) to get access to all of NetApp's Cloud offerings.
- Register for a [free trial](#) of Cloud Insights to explore the features available.
- **Subscribe** to Cloud Insights for on-going, uninterrupted access to your data via [NetApp Sales](#) direct or AWS Marketplace ([Standard Edition](#) or [Premium Edition](#)).

During the registration process, you can choose the global region to host your Cloud Insights environment. For more information, read about Cloud Insights [Information and Region](#).

Editions

The features and functionality available to you in Cloud Insights depend on the Edition to which you subscribe. The Editions available are explained here.

- **Basic Edition** is free and available to existing NetApp customers with an active NetApp support account.



Inactive Cloud Insights Basic Edition environments are deleted and their resources are reclaimed. An environment is considered inactive if there is no user activity for 30 consecutive days, or if there is no data ingested for 7 consecutive days. Cloud Insights will send a notification and provide a grace period of four days before an environment is deleted.



The features, data retention times, and objects or metrics collected in Cloud Insights Basic Edition are subject to change with or without notice.

- **Standard Edition** is available via subscription and offers all the features of Basic Edition plus more.
- **Premium Edition** offers additional benefits such as Business Intelligence and Reporting, as well as Workload Security Auditing and Threat Detection.

Key Features

Here are the key features available in Basic, Standard, and Premium Edition:

Key Feature	Basic Edition	Standard Edition	Premium Edition
Data Retention	7 Days	90 Days	13 Months
Infrastructure & Storage Metrics	NetApp Only	Multi-Vendor	Multi-Vendor
Customizable Dashboards	[check]	[check]	[check]
Forum, Documentation, and Training Videos	[check]	[check]	[check]
Live Chat and Technical Support	-	[check]	[check]
VM Metrics	-	[check]	[check]
Cloud Metrics	-	[check]	[check]

Service Metrics	-	[check]	[check]
Monitors and Alerting	*	[check]	[check]
API Access+	[check]	[check]	[check]
Single Sign-On (SSO)	-	-	[check]
Workload Security User Data Access Auditing	-	-	[check]
Workload Security Insider Threat Detection with AI/ML	-	-	[check]
Business Intelligence and Reporting**	-	-	[check]

*Limited to 5 active custom monitors at a time
 +API access varies by Edition
**Available for environments of 500 managed units and larger

While using Cloud Insights, if you see a padlock icon , it means the feature is not available in your current Edition, or is available in a limited form. Upgrade for full access to the feature.

Trial Version

When you sign up for Cloud Insights and your environment is active, you enter into a free, 30-day trial of Cloud Insights. During this trial you can explore the features that Cloud Insights has to offer, in your own environment.

At any time during your trial period, you can subscribe to Cloud Insights. Subscribing to Cloud Insights ensures uninterrupted access to your data as well as extended **product support** options.

Cloud Insights displays a banner when your free trial is nearing its end. Within that banner is a *View Subscription* link, which opens the **Admin > Subscription** page. Non-Admin users will see the banner but will not be able to go to the Subscription page.



If you need additional time to evaluate Cloud Insights and your trial is set to expire in 4 days or less, you can extend your trial for an additional 30 days. You can extend the trial only once. You cannot extend if your trial has expired.

Trial through AWS Marketplace

You may also sign up for a free trial through the AWS Marketplace. The AWS Marketplace free trial gives you access to Cloud Insights **Premium Edition** for a trial period of 33 days, and allows up to 499 **Managed Units** (MUs).

Note: If you configure more than 499 MUs, you will enter "breached" state. While your trial is in breached state, you will lose access to some Cloud Insights functionality until the breach is resolved, either by reducing the number of MUs configured, or by subscribing to Cloud Insights.

The AWS Marketplace free trial cannot be extended. At any time during your trial, you can downgrade to a Cloud Insights Basic Edition subscription or change to a paid Cloud Insights Standard or Premium Edition subscription by visiting the **Admin --> Subscription** page.

What if My Trial has Expired?

If your free trial has expired and you have not yet subscribed to Cloud Insights, you will have limited functionality until you subscribe.

Subscription Options

To subscribe, go to **Admin > Subscription**. In addition to the **Subscribe** buttons, you will be able to see your installed data collectors and calculate your estimated pricing. For a typical environment, you can click the self-serve AWS Marketplace **Subscribe Now** button. If your environment includes or is expected to include 1,000 or more Managed Units, you are eligible for Volume Pricing.

Key Features	Basic Free Available Only for NetApp Customers	Standard \$42 / mo* 7 Managed Units at \$6 MU/mo Billed Annually Contact Sales Or Subscribe Via Amazon Marketplace	Premium \$63 / mo* 7 Managed Units at \$9 MU/mo Billed Annually Contact Sales Or Subscribe Via Amazon Marketplace
Data Retention	7 Days	90 Days	13 Months
Infrastructure and Storage Metrics	NetApp Only	Multi-Vendor	Multi-Vendor
Customizable Dashboards	✓	✓	✓
Real-time Dashboards	✓	✓	✓
Forum, Documentation and Training Videos	✓	✓	✓
Live Chat and Technical Support	—	✓	✓
VM Metrics	—	✓	✓
Cloud Metrics	—	✓	✓
Service Metrics	—	✓	✓
Monitors and Alerting	—	✓	✓
API Access	—	—	✓
Single Sign-On (SSO)	—	—	✓
Cloud Secure User Data Access Auditing	—	—	✓
Cloud Secure Insider Threat Detection with AI/ML	—	—	✓
Business Intelligence and Reporting	—	—	Requires at least 500 MUs

Pricing

Cloud Insights is priced per **Managed Unit**. Usage of your Managed Units is calculated based on the number of **hosts or virtual machines** and amount of **unformatted capacity** being managed in your infrastructure environment.

- 1 Managed Unit = 2 hosts (any virtual or physical machine)
- 1 Managed Unit = 4 TiB of unformatted capacity of physical or virtual disks

Note that the following data collectors are metered at a different Raw TiB to Managed Unit rate. Every 40TiB of unformatted capacity on these data collectors is charged as 1 Managed Unit (MU):

- AWS S3
- Dell EMC ECS
- Hitachi Content Platform
- IBM Cleversafe
- NetApp StorageGrid

If your environment includes or is expected to include 1,000 or more Managed Units, you are eligible for **Volume Pricing** and will be prompted to Contact NetApp Sales to subscribe. See [below](#) for more details.

Estimate Your Subscription Cost

The Subscription Calculator gives you an estimated list-price monthly Cloud Insights cost based on the number of hosts and amount of unformatted capacity being reported by your data collectors. The current values are pre-populated in the *Hosts* and *Unformatted Capacity* fields. You can enter different values to assist you with planning for estimated future growth.

Your estimated list price cost will change based on your subscription term.



The calculator is for estimation only. Your exact pricing will be set when you subscribe.

How Do I Subscribe?

If your Managed Unit count is less than 1,000, you can subscribe via NetApp Sales, or [self-subscribe](#) via AWS Marketplace.

Subscribe through NetApp Sales direct

If your expected Managed Unit count is 1,000 or greater, click on the [Contact Sales](#) button to subscribe through the NetApp Sales Team.

You must provide your Cloud Insights **Serial Number** to your NetApp sales representative so that your paid subscription can be applied to your Cloud Insights environment. The Serial Number uniquely identifies your Cloud Insights trial environment and can be found on the [Admin > Subscription](#) page.

Self-Subscribe through AWS Marketplace



You must be an Account Owner or Administrator in order to apply an AWS Marketplace subscription to your existing Cloud Insights trial account. Additionally, you must have an Amazon Web Services (AWS) account.

Clicking on the **Subscribe Now** button opens the AWS [Cloud Insights](#) subscription page, where you can complete your subscription. Note that values you entered in the calculator are not populated in the AWS subscription page; you will need to enter the total Managed Units count on this page.

After you have entered the total Managed Units count and chosen either 12-month or 36-month subscription term, click on **Set Up Your Account** to finish the subscription process.

Once the AWS subscription process is complete, you will be taken back to your Cloud Insights environment. Or, if the environment is no longer active (for example, you have logged out), you will be taken to the Cloud Central sign-in page. When you sign in to Cloud Insights again, your subscription will be active.



After clicking on **Set Up Your account** on the AWS Marketplace page, you must complete the AWS subscription process within one hour. If you do not complete it within one hour, you will need to click on **Set Up Your Account** again to complete the process.

If there is a problem and the subscription process fails to complete correctly, you will still see the "Trial Version" banner when you log into your environment. In this event, you can go to **Admin > Subscription** and repeat the subscription process.

View Your Subscription Status

Once your subscription is active, you can view your subscription status and Managed Unit usage from the **Admin > Subscription** page.

The screenshot shows the AWS Subscription Details page. At the top, there are two tabs: "Subscription Details" (which is selected) and "Usage Management".

Active Entitlement Summary:

- NetApp Serial Number: 95030018085431676774
- Edition: Premium
- Total undefined Managed Units with some valid through February 8th, 2023

Modify Subscription:

- NetApp**: Enter an entitlement ID# or contact sales to modify your subscriptions.
- [Contact Sales to Modify Subscription](#)
- Estimate Cost**
- [+ Entitlement ID](#)

The Subscription Details tab displays the following:

- Current subscription or active Edition
- Details about your subscription
- Links to modify your subscription or estimate cost changes

View your Usage Management

The Usage Management tab shows an overview of Managed Unit usage, as well as a list of the Data Collectors installed in your environment and the breakdown of Managed Units for each.



The Unformatted Capacity Managed Unit count reflects a sum of the total raw capacity in the environment and is rounded up to the nearest Managed Unit.



The sum of Managed Units may differ slightly from the Data Collectors count in the summary section. This is because Managed Unit counts are rounded up to the nearest Managed Unit. The sum of these numbers in the Data Collectors list may be slightly higher than the total Managed Units in the status section. The summary section reflects your actual Managed Unit count for your subscription.

In the event that your usage is nearing or exceeding your subscribed amount, you can delete data collectors in this list by clicking on the "three dots" menu and selecting *Delete*.

What Happens if I Exceed My Subscribed Usage?

Warnings are displayed when your Managed Unit usage exceeds 80%, 90%, and 100% of your total subscribed amount:

When usage exceeds:	This happens / Recommended action:
80%	An informational banner is displayed. No action is necessary.
90%	A warning banner is displayed. You may want to increase your subscribed Managed Unit count.
100%	An error banner is displayed and you will have limited functionality until you do one of the following: * Modify your subscription to increase the subscribed Managed Unit count * Remove Data Collectors so that your Managed Unit usage is at or below your subscribed amount

Subscribe Directly and Skip the Trial

You can also subscribe to Cloud Insights directly from the [AWS Marketplace](#), without first creating a trial environment. Once your subscription is complete and your environment is set up, you will immediately be subscribed.

Adding an Entitlement ID

If you own a valid NetApp product that is bundled with Cloud Insights, you can add that product serial number to your existing Cloud Insights subscription. For example, if you have purchased NetApp Astra Control Center, the Astra Control Center license serial number can be used to identify the subscription in Cloud Insights. Cloud Insights refers to this as an *Entitlement ID*.

To add an entitlement ID to your Cloud Insights subscription, on the **Admin > Subscription** page, click **+Entitlement ID**.

Subscription Summary

NetApp Serial Number: 95001014387268156333
Active Edition: Premium
[+ Entitlement ID](#)

Usage and Entitlement

5,122 out of 18,000 Managed Units



Hosts: 1,388 Managed Units (2,776 Hosts)

Unformatted Capacity: 3,734 Managed Units (14,934 TB)

Subscription Details

36 Months (Premium Edition)

Expires: March 3rd, 2022



[Modify Subscription](#)

[Estimate Cost](#)

Automatic Device Resolution

Automatic Device Resolution Overview

You need to identify all of the devices you want to monitor with Cloud Insights.

Identification is necessary in order to accurately track performance and inventory in your environment. Typically the majority of devices discovered in your environment are identified through *Automatic Device Resolution*.

After you configure data collectors, devices in your environment including switches, storage arrays, and your virtual infrastructure of hypervisors and VMs are identified. However, this does not normally identify 100% of the devices in your environment.

After data collector type devices have been configured, best practice is to leverage device resolution rules to help identify the remaining unknown devices in your environment. Device resolution can help you resolve unknown devices as the following device types:

- Physical hosts
- Storage arrays
- Tapes

Devices remaining as unknown after device resolution are considered generic devices, which you can also show in queries and on dashboards.

The rules created in turn will automatically identify new devices with similar attributes as they are added to your environment. In some cases, device resolution also allows for manual identification bypassing the device resolution rules for undiscovered devices within Cloud Insights.

Incomplete identification of devices can result in issues including:

- Incomplete paths
- Unidentified multipath connections
- The inability to group applications
- Inaccurate topology views
- Inaccurate data in the Data warehouse and reporting

The device resolution feature (Manage > Device resolution) includes the following tabs, each of which plays a role in device resolution planning and viewing results:

- **Fibre Channel Identify** contains a list WWNs and port information of Fibre Channel devices that were not resolved through automatic device resolution. The tab also identifies the percentage of devices that have been identified.
- **IP Address Identify** contains a list of devices accessing CIFS shares and NFS shares that were not identified through automatic device resolution. The tab also identifies the percentage of devices that have been identified.
- **Auto resolution rules** contains the list of rules that are run when performing Fibre channel device resolution. These are rules you create to resolve unidentified Fibre channel devices.
- **Preferences** provides configuration options that you use to customize device resolution for your

environment.

Before You Begin

You need to know how your environment is configured before you define the rules for identifying devices. The more you know about your environment the easier it will be to identify devices.

You need to answer questions similar to the following to help you create accurate rules:

- Does your environment have naming standards for zones or hosts and what percentage of these are accurate?
- Does your environment use a switch alias or storage alias and do they match the host name?
- How often do naming schemes change in your environment?
- Have there been any acquisitions or mergers that introduced different naming schemes?

After analyzing your environment, you should be able to identify what naming standards exist that you can expect to reliability encounter. The information you gathered might be represented graphically in a figure similar to the following:



In this example the largest number of devices are reliably represented by storage aliases. Rules that identify hosts using storage aliases should be written first, rules using switch aliases should be written next , and the last rules created should use zone aliases. Due to the overlap of the use of zone aliases and switch aliases, some storage alias rules might identify additional devices, leaving less rules required for zone aliases and switch aliases.

Steps to Identifying devices

Typically, you would use a workflow similar to the following to identify devices in your environment. Identification is an iterative process and might require multiple steps of planning and refining rules.

- Research environment
- Plan rules
- Create/Revise rules
- Review results
- Create additional rules or Manually Identify devices
- Done



If you have unidentified devices (otherwise known as unknown or generic devices) in your environment and you subsequently configure a data source that identifies those devices upon polling, they will no longer be displayed or counted as generic devices.

Related:

[Creating Device Resolution Rules](#)

[Fibre Channel Device Resolution](#)

[IP Device Resolution](#)

[Setting Device Resolution Preferences](#)

Device Resolution rules

You create device resolution rules to identify hosts, storage, and tapes that are not automatically identified currently by Cloud Insights. The rules that you create identify devices currently in your environment and also identify similar devices as they are added to your environment.

Creating Device Resolution Rules

When you create rules you start by identifying the source of information that the rule runs against, the method used to extract information, and whether DNS lookup is applied to the results of the rule.

Source that is used to identify the device	* SRM aliases for hosts * Storage alias containing an embedded host or tape name * Switch alias containing an embedded host or tape name * Zone names containing an embedded host name
Method that is used to extract the device name from the source	* As is (extract a name from an SRM) * Delimiters * Regular expressions
DNS lookup	Specifies if you use DNS to verify the host name

You create rules in the Auto Resolution Rules tab. The following steps describe the rule creation process.

Procedure

1. Click **Manage > Device Resolution**
2. In the **Auto resolution rules** tab, click **+ Host Rule** or **+ Tape Rule**.

The **Resolution Rule** screen is displayed.



Click the *View matching criteria* link for help with and examples for creating regular expressions.

3. In the **Type** list select the device you want to identify.

You can select *Host* or *Tape*.

4. In the **Source** list, select the source you want to use to identify the host.

Depending on the source you chose, Cloud Insights displays the following response:

- Zones** lists the zones and WWN that need to be identified by Cloud Insights.
 - SRM** lists the unidentified aliases that need to be identified by Cloud Insights
 - Storage alias** lists storage aliases and WWN that need to be identified by Cloud Insights
 - Switch alias** lists the switch aliases that need to be identified by Cloud Insights
5. In the **Method** list select the method you want to employ to identify the host.

Source	Method
SRM	As is, Delimiters, Regular expressions
Storage alias	Delimiters, Regular expressions
Switch alias	Delimiters, Regular expressions
Zones	Delimiters, Regular expressions

- Rules using Delimiters require the delimiters and the minimum length of the host name. The minimum length of the host name is number of characters that Cloud Insights should use to identify a host. Cloud Insights performs DNS lookups only for host names that are this long or longer.

For rules using Delimiters, the input string is tokenized by the delimiter and a list of host name candidates is created by making several combinations of the adjacent token. The list is then sorted, largest to smallest. For example, for an input string of *vipsnq03_hba3_emc3_12ep0* the list would result in the following:

- *vipsnq03_hba3_emc3_12ep0*
- *vipsnq03_hba3_emc3*
- *hba3 emc3_12ep0*
- *vipsnq03_hba3*
- *emc3_12ep0*
- *hba3_emc3*
- *vipsnq03*
- *12ep0*

- emc3
 - hba3
- Rules using Regular expressions require a regular expression, the format, and cases sensitivity selection.
6. Click **Run AR** to run all rules, or click the down-arrow in the button to run the rule you created (and any other rules that have been created since the last full run of AR).

The results of the rule run are displayed in the **FC identify** tab.

Starting an automatic device resolution update

A device resolution update commits manual changes that have been added since the last full automatic device resolution run. Running an update can be used to commit and run only the new manual entries made to the device resolution configuration. No full device resolution run is performed.

Procedure

1. Log into the Cloud Insights web UI.
2. Click **Manage > Device Resolution**
3. In the **Device Resolution** screen, click the down-arrow in the **Run AR** button.
4. Click **Update** to start the update.

Rule-assisted manual identification

This feature is used for special cases where you want to run a specific rule or a list of rules (with or without a one-time reordering) to resolve unknown hosts, storage, and tape devices.

Before you begin

You have a number of devices that have not been identified and you also have multiple rules that successfully identified other devices.



If your source only contains part of a host or device name, use a regular expression rule and format it to add the missing text.

Procedure

1. Log into the Cloud Insights web UI.
2. Click **Manage > Device Resolution**
3. Click the **Fibre Channel Identify** tab.

The system displays the devices along with their resolution status.

4. Select multiple unidentified devices.
5. Click **Bulk Actions** and select **Set host resolution** or **Set tape resolution**.

The system displays the Identify screen which contains a list of all of the rules that successfully identified devices.

6. Change the order of the rules to an order that meets your needs.

The order of the rules are changed in the Identify screen, but are not changed globally.

7. Select the method that that meets your needs.

Cloud Insights executes the host resolution process in the order in which the methods appear, beginning with those at the top.

When rules that apply are encountered, rule names are shown in the rules column and identified as manual.

Related:

[Fibre Channel Device Resolution](#)

[IP Device Resolution](#)

[Setting Device Resolution Preferences](#)

Fibre Channel device resolution

The Fibre Channel Identify screen displays the WWN and WWPN of fibre channel devices whose hosts have not been identified by automatic device resolution. The screen also displays any devices that have been resolved by manual device resolution.

Devices that have been resolved by manual resolution contain a status of *OK* and identify the rule used to identify the device. Missing devices have a status of *Unidentified*. Devices that are specifically excluded from identification have a status of *Excluded*. The total coverage for identification of devices is listed on this page.

You perform bulk actions by selecting multiple devices on the left-hand side of the Fibre Channel Identify screen. Actions can be performed on a single device by hovering over a device and selecting the *Identify* or *Unidentify* buttons on the far right of the list.

The *Total Coverage* link displays a list of the number of devices identified/number of devices available for your configuration:

- SRM alias
- Storage alias
- Switch alias
- Zones
- User defined

Adding a Fibre Channel device manually

You can manually add a fibre channel device to Cloud Insights using the *Manual Add* feature available in the device resolution Fibre Channel Identify tab. This process might be used for pre-identification of a device that is expected to be discovered in the future.

Before you begin

To successfully add a device identification to the system you need to know the WWN or IP address and the device name.

About this task

You can add a Host, Storage, Tape or Unknown fibre channel device manually.

Procedure

1. Log in to the Cloud Insights web UI

2. Click **Manage > Device Resolution**
3. Click the **Fibre Channel Identify** tab.
4. Click the **Add** button.

The **Add Device** dialog is displayed

5. Enter the WWN or IP address, the device name, and select the device type.

The device you enter is added to the list of devices in the Fibre Channel Identify tab. The Rule is identified as *Manual*.

Importing Fibre Channel device identification from a .CSV file

You can manually import fibre channel device identification into Cloud Insights device resolution using a list of devices in a .CSV file.

1. Before you begin

You must have a correctly formatted .CSV file in order to import device identifications directly into device resolution. The .CSV file for fibre channel devices requires the following information:

WWN	IP	Name	Type
-----	----	------	------

The data fields must be enclosed in quotes, as shown in the example below.

```
"WWN", "IP", "Name", "Type"
"WWN:2693", "ADDRESS2693|IP2693", "NAME-2693", "HOST"
"WWN:997", "ADDRESS997|IP997", "NAME-997", "HOST"
"WWN:1860", "ADDRESS1860|IP1860", "NAME-1860", "HOST"
```



As a best practice, it is recommended to first export the Fibre Channel Identify information to a .CSV file, make your desired changes in that file, and then import the file back into Fibre Channel Identify. This ensures that the expected columns are present and in the proper order.

To import Fibre Channel Identify information:

1. Log into the Cloud Insights web UI.
2. Click **Manage > Device Resolution**
3. Select the **Fibre Channel Identify** tab.
4. Click the **Identify > Identify from file** button.
5. Navigate to the folder containing your .CSV files for import and select the desired file.

The devices you enter are added to the list of devices in the Fibre Channel Identify tab. The “Rule” is identified as *Manual*.

Exporting Fibre Channel device identifications to a .CSV file

You can export existing fibre channel device identifications to a .CSV file from the Cloud Insights device resolution feature. You might want to export a device identification so that you can modify it and then import it back into Cloud Insights where it is then used to identify devices that are similar to those originally matching the exported identification.

About this task

This scenario might be used when devices have similar attributes that can be easily edited in the .CSV file and then imported back into the system.

When you export a Fibre Channel device identification to a .CSV file, the file contains the following information in the order shown:

WWN	IP	Name	Type
-----	----	------	------

Procedure

1. Log into the Cloud Insights web UI.
2. Click **Manage > Device Resolution**
3. Select the **Fibre Channel Identify** tab.
4. Select the Fibre Channel device or devices whose identification you want to export.
5. Click the **Export**  button.

Select whether to open the .CSV file or save the file.

Related:

[IP Device Resolution](#)

[Creating Device Resolution Rules](#)

[Setting Device Resolution Preferences](#)

IP device resolution

The IP Identify screen displays any iSCSI and CIFS or NFS shares that have been identified by automatic device resolution or by manual device resolution. Unidentified devices are also shown. The screen includes the IP address, Name, Status, iSCSI node, and share name for devices. The percentage of devices that have been successfully identified is also displayed.

IP identify (10)						Total coverage 20% (2/10)
	Address	IP	Name	Status	iSCSI node	Share name
<input type="checkbox"/>	1.1.1.1	1.1.1.1	LA3-CNS-SQL-06A	OK		\vol\ServerLogs_STG\
<input type="checkbox"/>	0.0.0.0/0					\vol\ServerLogs_STG\
<input type="checkbox"/>	10.56.100.18				iqn.1991-05.com.microsoft\la3-cns-sql-06b.cns.comcastnets.com	
<input type="checkbox"/>	10.56.100.19				iqn.1991-05.com.microsoft\jec20643597717.tfayd.com	\vol\wc_sc_libraries_prod\libraries_qtree\
<input type="checkbox"/>	100.54.18.100	100.54.18.100	ushapiip00096lb	OK		

Adding IP devices manually

You can manually add an IP device to Cloud Insights using the manual add feature available in the IP Identify screen.

Procedure

1. Log in to the Cloud insights web UI.
2. Click **Manage > Device resolution**
3. Click the **IP Address Identify** tab.
4. Click the **Add** button.

The Add Device dialog is displayed

5. Enter the address, IP address, and a unique device name.

Result

The device you enter is added to the list of devices in the IP Address Identify tab.

Importing IP device identification from a .CSV file

You can manually import IP device identifications into the Device Resolution feature using a list of device identifications in a .CSV file.

1. Before you begin

You must have a correctly formatted .CSV file in order to import device identifications directly into the Device Resolution feature. The .CSV file for IP devices requires the following information:

Address	IP	Name
---------	----	------

The data fields must be enclosed in quotes, as shown in the example below.

```
"Address","IP","Name"  
"ADDRESS6447","IP6447","NAME-6447"  
"ADDRESS3211","IP3211","NAME-3211"  
"ADDRESS593","IP593","NAME-593"
```



As a best practice, it is recommended to first export the IP Address Identify information to a .CSV file, make your desired changes in that file, and then import the file back into IP Address Identify. This ensures that the expected columns are present and in the proper order.

Exporting IP device identification to a .CSV file

You can export existing IP device identifications to a .CSV file from the Cloud Insights device resolution feature. You might want to export a device identification so that you can modify it and then import it back into Cloud Insights where it is then used to identify devices that are similar to those originally matching the exported identification.

About this task

This scenario might be used when devices have similar attributes that can be easily edited in the .CSV file and then imported back into the system.

When you export an IP device identification to a .CSV file, the file contains the following information in the order shown:

Address	IP	Name
---------	----	------

Procedure

1. Log into the Cloud Insights web UI.
2. Click **Manage > Device Resolution**
3. Select the **IP Address Identify** tab.
4. Select the IP device or devices whose identification you want to export.
5. Click the **Export**  button.

Select whether to open the .CSV file or save the file.

Related:

[Fibre Channel device resolution](#)

[Creating Device Resolution Rules](#)

[Setting Device Resolution Preferences](#)

Setting options in the Preferences tab

The device resolution preferences tab lets you create an auto resolution schedule, specify storage and tape vendors to include or exclude from identification, and set DNS lookup options.

Auto resolution schedule

An auto resolution schedule can specify when automatic device resolution is run:

Option	Description
Every	Use this option to run automatic device resolution on intervals of days, hours, or minutes.
Every day	Use this option to run automatic device resolution daily at a specific time.
Manually	Use this option to only run automatic device resolution manually.
On every environment change	Use this option to run automatic device resolution whenever there is a change in the environment.

If you specify *Manually*, nightly automatic device resolution is disabled.

DNS processing options

DNS processing options allow you to select the following features:

- When DNS lookup result processing is enabled, you can add a list of DNS names to append to resolved devices.
- You can select Auto resolution of IPs: to enables automatic host resolution for iSCSI initiators and hosts accessing NFS shares by using DNS lookup. If this is not specified, only FC-based resolution is performed.
- You can choose to allow underscores in host names and to use a "connected to" alias instead of the standard port alias in results.

Including or excluding specific storage and tape vendors

You can include or exclude specific storage and tape vendors for automatic resolution. You might want to exclude specific vendors if you know, for example, that a specific host will become a legacy host and should be excluded from your new environment. You can also re-add vendors that you earlier excluded but no longer want excluded.



Device resolution rules for tape only work for WWNs where the Vendor for that WWN is set to *Included as Tape only* in the Vendors preferences.

See also: [Regular Expression Examples](#)

Regular expression examples

If you have selected the regular expression approach as your source naming strategy, you can use the regular expression examples as guides for your own expressions used in the Cloud Insights automatic resolution methods.

Formatting regular expressions

When creating regular expressions for Cloud Insights automatic resolution, you can configure output format by entering values in a field named *FORMAT*.

The default setting is \1, which means that a zone name that matches the regular expression is replaced by the contents of the first variable created by the regular expression. In a regular expression, variable values are created by parenthetical statements. If multiple parenthetical statements occur, the variables are referenced numerically, from left to right. The variables can be used in the output format in any order. Constant text can also be inserted in the output, by adding it to the *FORMAT* field.

For example, you might have the following zone names for this zone naming convention:

```
[Zone number]_[data center]_[hostname]_[device type]_[interface number]
```

- S123_Miami_hostname1_filer_FC1
- S14_Tampa_hostname2_switch_FC4
- S3991_Boston_hostname3_windows2K_FC0
- S44_Raleigh_hostname4_solaris_FC1

And you might want the output to be in the following format:

```
[hostname]-[data center]-[device type]
```

To do this, you need to capture the host name, data center, and device type fields in variables, and use them in the output. The following regular expression would do this:

```
. *? _ ([a-zA-Z0-9]+) _ ([a-zA-Z0-9]+) _ ([a-zA-Z0-9]+) _ *
```

Because there are three sets of parentheses, the variables \1, \2 and \3 would be populated.

You could then use the following format to receive output in your preferred format:

```
\2-\1-\3
```

Your output would be as follows:

```
hostname1-Miami-filer  
hostname2-Tampa-switch  
hostname3-Boston-windows2K  
hostname4-Raleigh-solaris
```

The hyphens between the variables provide an example of constant text that is inserted in the formatted output.

Examples

Example 1 showing zone names

In this example, you use the regular expression to extract a host name from the zone name. You could create a regular expression if you have something similar to the following zone names:

- S0032_myComputer1Name-HBA0
- S0434_myComputer1Name-HBA1
- S0432_myComputer1Name-HBA3

The regular expression that you could use to capture the host name would be:

```
S [0-9]+_ ([a-zA-Z0-9]*) [-] HBA [0-9]
```

The outcome is a match of all zones beginning with S that are followed by any combination of digits , followed by an underscore, the alphanumeric hostname (myComputer1Name), an underscore or hyphen, the capital letters HBA, and a single digit (0-9). The hostname alone is stored in the \1 variable.

The regular expression can be broken into its components:

- "S" represents the zone name and begins the expression. This matches only an "S" at the beginning of the zone name.
- The characters [0-9] in brackets indicate that what follows "S" must be a digit between 0 and 9, inclusive.
- The + sign indicates that the occurrence of the information in the preceding brackets has to exist 1 or more times.
- The _ (underscore) means that the digits after S must be followed immediately by only an underscore character in the zone name. In this example, the zone naming convention uses the underscore to separate the zone name from the host name.
- After the required underscore, the parentheses indicate that the pattern contained within will be stored in the \1 variable.
- The bracketed characters [a-zA-Z0-9] indicate that the characters being matched are all letters (regardless of case) and numbers.
- The * (asterisk) following the brackets indicates that the bracketed characters occur 0 or more times.
- The bracketed characters [-] (underscore and dash) indicate that the alphanumeric pattern must be followed by an underscore or a dash.
- The letters HBA in the regular expression indicate that this exact sequence of characters must occur in the zone name.
- The final set of bracketed characters [0-9] match a single digit from 0 through 9, inclusive.

Example 2

In this example, skip up to the first underscore "", then match E and everything after that up to the second "", and then skip everything after that.

Zone: Z_E2FHDBS01_E1NETAPP

Hostname: E2FHDBS01

RegExp: .?(E.?).*?

Example 3

The parentheses "()" around the last section in the Regular Expression (below) identifies which part is the hostname. If you wanted VSAN3 to be the host name, it would be: _([a-zA-Z0-9]).*

Zone: A_VSAN3_SR48KENT_A_CX2578_SPA0

Hostname: SR48KENT

RegExp: _[a-zA-Z0-9]+_([a-zA-Z0-9]).*

Example 4 showing a more complicated naming pattern

You could create a regular expression if you have something similar to the following zone names:

- myComputerName123-HBA1_Symm1_FA3
- myComputerName123-HBA2_Symm1_FA5
- myComputerName123-HBA3_Symm1_FA7

The regular expression that you could use to capture these would be:

```
( [a-zA-Z0-9]* ) _.*
```

The \1 variable would contain only *myComputerName123* after being evaluated by this expression.

The regular expression can be broken into its components:

- The parentheses indicate that the pattern contained within will be stored in the \1 variable.
- The bracketed characters [a-zA-Z0-9] mean that any letter (regardless of case) or digit will match.
- The * (asterisk) following the brackets indicates that the bracketed characters occur 0 or more times.
- The _ (underscore) character in the regular expression means that the zone name must have an underscore immediately following the alphanumeric string matched by the preceding brackets.
- The . (period) matches any character (a wildcard).
- The * (asterisk) indicates that the preceding period wildcard may occur 0 or more times.

In other words, the combination .* indicates any character, any number of times.

Example 5 showing zone names without a pattern

You could create a regular expression if you have something similar to the following zone names:

- myComputerName_HBA1_Symm1_FA1
- myComputerName123_HBA1_Symm1_FA1

The regular expression that you could use to capture these would be:

```
( .*? ) _.*
```

The \1 variable would contain *myComputerName* (in the first zone name example) or *myComputerName123* (in the second zone name example). This regular expression would thus match everything prior to the first underscore.

The regular expression can be broken into its components:

- The parentheses indicate that the pattern contained within will be stored in the \1 variable.
- The .* (period asterisk) match any character, any number of times.
- The * (asterisk) following the brackets indicates that the bracketed characters occur 0 or more times.
- The ? character makes the match non-greedy. This forces it to stop matching at the first underscore, rather than the last.
- The characters _.* match the first underscore found and all characters that follow it.

Example 6 showing computer names with a pattern

You could create a regular expression if you have something similar to the following zone names:

- Storage1_Switch1_myComputerName123A_A1_FC1
- Storage2_Switch2_myComputerName123B_A2_FC2
- Storage3_Switch3_myComputerName123T_A3_FC3

The regular expression that you could use to capture these would be:

```
. * ? _ . * ? _ ( [ a - z A - Z 0 - 9 ] * [ ABT ] ) _ . *
```

Because the zone naming convention has more of a pattern, we could use the above expression, which will match all instances of a hostname (myComputerName in the example) that ends with either an A, a B, or a T, placing that hostname in the \1 variable.

The regular expression can be broken into its components:

- The .* (period asterisk) match any character, any number of times.
- The ? character makes the match non-greedy. This forces it to stop matching at the first underscore, rather than the last.
- The underscore character matches the first underscore in the zone name.
- Thus, the first .*?_ combination matches the characters Storage1_ in the first zone name example.
- The second .*?_ combination behaves like the first, but matches Switch1_ in the first zone name example.
- The parentheses indicate that the pattern contained within will be stored in the \1 variable.
- The bracketed characters [a-zA-Z0-9] mean that any letter (regardless of case) or digit will match.
- The * (asterisk) following the brackets indicates that the bracketed characters occur 0 or more times.
- The bracketed characters in the regular expression [ABT] match a single character in the zone name which must be A, B, or T.
- The _(underscore) following the parentheses indicates that the [ABT] character match must be followed up an underscore.
- The .* (period asterisk) match any character, any number of times.

The result of this would therefore cause the \1 variable to contain any alphanumeric string which:

- was preceded by some number of alphanumeric characters and two underscores
- was followed by an underscore (and then any number of alphanumeric characters)
- had a final character of A, B or T, prior to the third underscore.

Example 7

Zone: myComputerName123_HBA1_Symm1_FA1

Hostname: myComputerName123

RegExp: ([a-zA-Z0-9]+)_.*

Example 8

This example finds everything before the first _.

Zone: MyComputerName_HBA1_Symm1_FA1

MyComputerName123_HBA1_Symm1_FA1

Hostname: MyComputerName

RegExp: (.?)_.

Example 9

This example finds everything after the 1st _ and up to the second _.

Zone: Z_MyComputerName_StorageName

Hostname: MyComputerName

RegExp: .?(.?).*?

Example 10

This example extracts "MyComputerName123" from the zone examples.

Zone: Storage1_Switch1_MyComputerName123A_A1_FC1

Storage2_Switch2_MyComputerName123B_A2_FC2

Storage3_Switch3_MyComputerName123T_A3_FC3

Hostname: MyComputerName123

RegExp: .?.?([a-zA-Z0-9]+)[ABT]_.

Example 11

Zone: Storage1_Switch1_MyComputerName123A_A1_FC1

Hostname: MyComputerName123A

RegExp: .?.?([a-zA-Z0-9]+).*?

Example 12

The ^ (circumflex or caret) **inside square brackets** negates the expression, for example, [^Ff] means anything except uppercase or lowercase F, and [^a-z] means everything except lowercase a to z, and in the case above, anything except the _. The format statement adds in the "-" to the output host name.

Zone: mhs_apps44_d_A_10a0_0429

Hostname: mhs-apps44-d

RegExp: ()_([AB]).*Format in Cloud Insights: \1-\2 (\[^_])_()
()_([^_]).*Format in Cloud Insights: \1-\2-\3

Example 13

In this example, the storage alias is delimited by "\" and the expression needs to use "\\\" to define that there are actually "\\" being used in the string, and that those are not part of the expression itself.

Storage Alias: \\Hosts\\E2DOC01C1\\E2DOC01N1

Hostname: E2DOC01N1

RegExp: \\.?\\\\.?\\(.*)?

Example 14

This example extracts "PD-RV-W-AD-2" from the zone examples.

Zone: PD_D-PD-RV-W-AD-2_01

Hostname: PD-RV-W-AD-2

RegExp: -(.*-\d).*

Example 15

The format setting in this case adds the "US-BV-" to the hostname.

Zone: SRV_USBVM11_F1

Hostname: US-BV-M11

RegExp: SRV_USBV([A-Za-z0-9]+)_F[12]

Format: US-BV-\1

Creating Dashboards

Dashboards Overview

Cloud Insights provides users the flexibility to create operational views of infrastructure data, by allowing you to create custom dashboards with a variety of widgets, each of which provides extensive flexibility in displaying and charting your data.



The examples in these sections are for explanation purposes only and do not cover every possible scenario. The concepts and steps herein can be used to create your own dashboards to highlight the data specific to your particular needs.

Creating a Dashboard

You create a new dashboard in one of two places:

- **Dashboards > [+New dashboard]**
- **Dashboards > Show all dashboards > click the [+Dashboard] button**

Dashboard Controls

The Dashboard screen has several controls:

- **Time selector:** allows you to view dashboard data for a range of time from the last 15 minutes to the last 30 days, or a custom time range of up to 31 days. You can choose to override this global time range in individual widgets.
- **Edit button:** Selecting this will enable Edit mode, which allows you to make changes to the dashboard. New dashboards open in Edit mode by default.
- **Save button:** Allows you to save or delete the dashboard.

You can rename the current dashboard by typing a new name before clicking **Save**.

- **Add Widget button**, which allows you to add any number of tables, charts, or other widgets to the dashboard.

Widgets can be resized and relocated to different positions within the dashboard, to give you the best view of your data according to your current needs.

Widget types

You can choose from the following widget types:

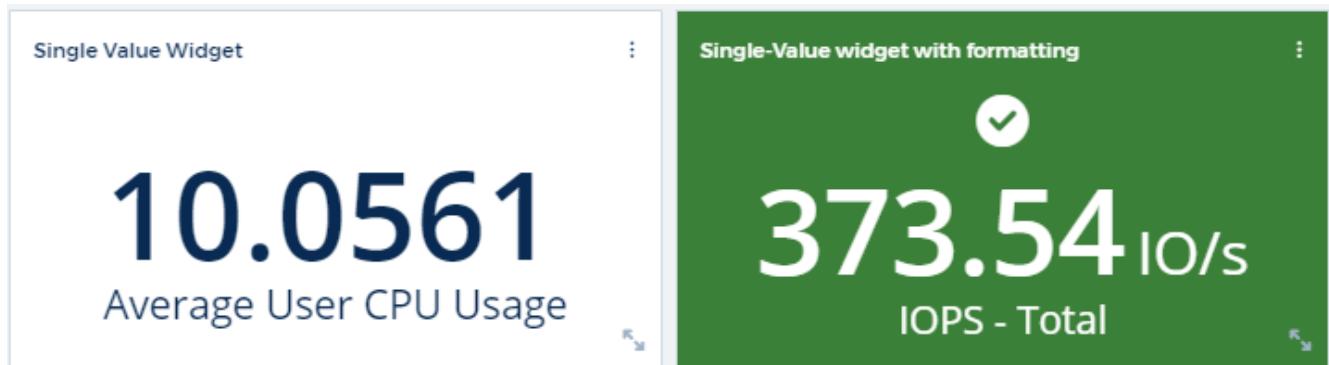
- **Table widget:** A table displaying data according to filters and columns you choose. Table data can be combined in groups that can be collapsed and expanded.

4 items found in 2 groups

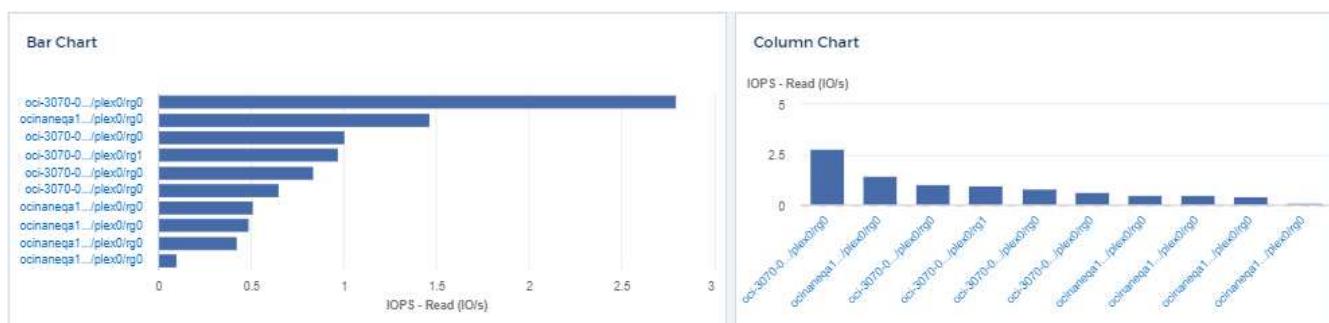
Active Date	Storage Node	Cache Hit Ratio - Total (%)	IOPS - Total (IO...)	IOPS - Write (I...)	Latency
06/01/2020 (1)	ocinaneqa1-01	N/A	N/A	N/A	N/A
06/01/2020	ocinaneqa1-01	N/A	N/A	N/A	N/A
N/A (3)	--	N/A	N/A	N/A	N/A

- **Line, Spline, Area, Stacked Area Charts:** These are time-series chart widgets on which you can display performance and other data over time.

- **Single Value widget:** A widget allowing you to display a single value that can be derived either directly from a counter or calculated using a query or expression. You can define color formatting thresholds to show whether the value is in expected, warning, or critical range.



- **Gauge widget:** Displays single-value data in a traditional (solid) gauge or bullet gauge, with colors based on "Warning" or "Critical" values you [customize](#).
- **Bar, Column Charts:** Displays top or bottom N values, for example, Top 10 storages by capacity or bottom 5 volumes by IOPS.



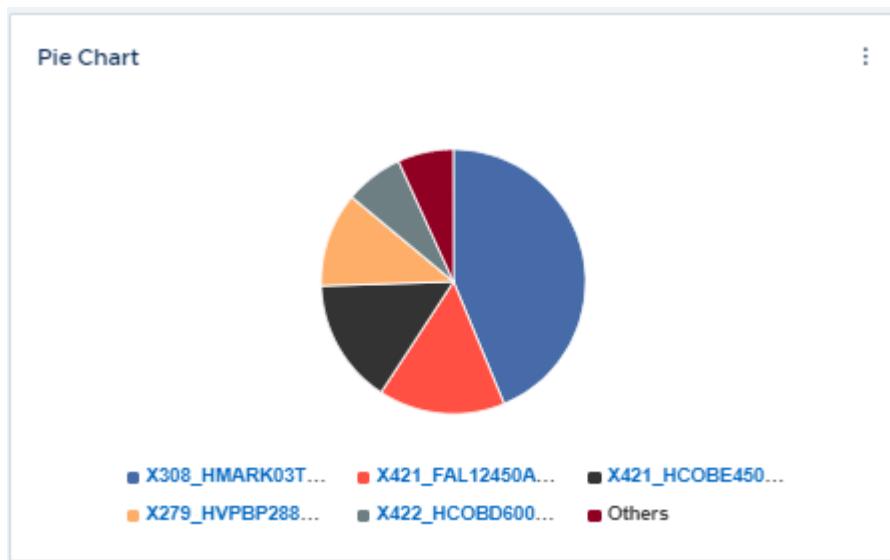
- **Box Plot Chart:** A plot of the min, max, median, and the range between lower and upper quartile of data in a single chart.



- **Scatter Plot Chart:** Plots related data as points, for example, IOPS and latency. In this example, you can quickly locate assets with high throughput and low IOPS.



- **Pie Chart:** a traditional pie chart to display data as a piece of the total.



- **Note widget:** Up to 1000 characters of free text.

Note Widget (with link)

This is a note. You can type any text you like in here, for example, to give details about the purpose of a particular dashboard.

You can also include [links](#) in your note.

- **Alerts Table:** Displays up to the last 1,000 alerts.

For more detailed explanations of these and other Dashboard Features, [click here](#).

Setting a Dashboard as your Home Page

You can choose which dashboard to set as your environment's **home page** using either of the following methods:

- Go to **Dashboards > Show All Dashboards** to display the list of dashboards in your environment. Click on the options menu to the right of the desired dashboard and select **Set as Home Page**.
- Click on a dashboard from the list to open the dashboard. Click the drop-down menu in the upper corner and select **Set as Home Page**.

Dashboard Features

Dashboards and widgets allow great flexibility in how data is displayed. Here are some concepts to help you get the most from your custom dashboards.

Widget Naming

Widgets are automatically named based on the object, metric, or attribute selected for the first widget query. If you also choose a grouping for the widget, the "Group by" attributes are included in the automatic naming (aggregation method and metric).

Average cpu.time_idle by agent_node_ip

agent.node.cpu.time_idle X + Display Unit: cpu.time_idle (None)

Display Last 3 Hours (Dashboard Time) X + Rolled up in segments of 1 minutes aggregated by Average X Edit Override Dashboard Time

Filter by Attribute X + Filter by Metric X +

Group by agent_node_ip X + aggregated by Average X + Apply f(x) Rank Top X + 10 X +

Cancel Save

Selecting a new object or grouping attribute updates the automatic name.

If you do not want to use the automatic widget name, you can simply type a new name.

Widget Placement and Size

All dashboard widgets can be positioned and sized according to your needs for each particular dashboard.

Duplicating a Widget

In dashboard Edit mode, click the menu on the widget and select **Duplicate**. The widget editor is launched, pre-filled with the original widget's configuration and with a "copy" suffix in the widget name. You can easily make any necessary changes and Save the new widget. The widget will be placed at the bottom of your dashboard, and you can position it as needed. Remember to Save your dashboard when all changes are complete.



Displaying Widget Legends

Most widgets on dashboards can be displayed with or without legends. Legends in widgets can be turned on or off on a dashboard by either of the following methods:

- When displaying the dashboard, click the **Options** button on the widget and select **Show Legends** in the menu.

As the data displayed in the widget changes, the legend for that widget is updated dynamically.

When legends are displayed, if the landing page of the asset indicated by the legend can be navigated to, the legend will display as a link to that asset page. If the legend displays "all", clicking the link will display a query page corresponding to the first query in the widget.

Transforming Metrics

Cloud Insights provides different **transform** options for certain metrics in widgets (specifically, those metrics called "Custom" or Integration Metrics, such as from Kubernetes, ONTAP Advanced Data, Telegraf plugins, etc.), allowing you to display the data in a number of ways. When adding transformable metrics to a widget, you are presented with a drop-down giving the following transform choices:

None

Data is displayed as is, with no manipulation.

Rate

Current value divided by the time range since the previous observation.

Cumulative

The accumulation of the sum of previous values and the current value.

Delta

The difference between the previous observation value and the current value.

Delta rate

Delta value divided by the time range since the previous observation.

Cumulative Rate

Cumulative value divided by the time range since the previous observation.

Note that transforming metrics does not change the underlying data itself, but only the way that data is displayed.

Dashboard widget queries and filters

Queries

The Query in a dashboard widget is a powerful tool for managing the display of your data. Here are some things to note about widget queries.

Some widgets can have up to five queries. Each query will plot its own set of lines or graphs in the widget. Setting rollup, grouping, top/bottom results, etc. on one query does not affect any other queries for the widget.

You can click on the eye icon to temporarily hide a query. The widget display updates automatically when you hide or show a query. This allows you to check your displayed data for individual queries as you build your widget.

The following widget types can have multiple queries:

- Area chart
- Stacked area chart
- Line chart
- Spline chart
- Single value widget

The remaining widget types can have only a single query:

- Table
- Bar chart
- Box plot
- Scatter plot

Filtering in dashboard widget queries

Here are some things you can do to get the most out of your filters.

Exact Match Filtering

If you enclose a filter string in double quotes, Insight treats everything between the first and last quote as an exact match. Any special characters or operators inside the quotes will be treated as literals. For example, filtering for "*" will return results that are a literal asterisk; the asterisk will not be treated as a wildcard in this case. The operators AND, OR, and NOT will also be treated as literal strings when enclosed in double quotes.

You can use exact match filters to find specific resources, for example hostname. If you want to find only the hostname 'marketing' but exclude 'marketing01', 'marketing-boston', etc., simply enclose the name "marketing" in double quotes.

Wildcards and Expressions

When you are filtering for text or list values in queries or dashboard widgets, as you begin typing you are presented with the option to create a **wildcard filter** based on the current text. Selecting this option will return all results that match the wildcard expression. You can also create **expressions** using NOT or OR, or you can select the "None" option to filter for null values in the field.

kubernetes.pod X ▼

Filter By pod_name ingest ▼ X + ?

Group pod_name X

Create wildcard containing "ingest"

ci-service-datalake-ingestion-85b5bdfd6d-2qbwr

service-foundation-ingest-767dfd5bfc-vxd5p

None

71 items found

Table Row Grouping

Filters based on wildcards or expressions (e.g. NOT, OR, "None", etc.) display in dark blue in the filter field. Items that you select directly from the list are displayed in light blue.

The screenshot shows a dashboard interface with a search bar at the top containing the text "kubernetes.pod". Below the search bar are several filter buttons: "Filter By pod_name *ingest*", "ci-service-audit-5f775dd975-brfdc", and a "Group pod_name" button. The main area displays a table titled "Table Row Grouping" with one column labeled "pod_name". The table contains three rows of data: "ci-service-audit-5f775dd975-brfdc", "ci-service-datalake-ingestion-85b5bdfd6d-2qbwr", and "service-foundation-ingest-767dfd5bfc-vxd5p".

pod_name
ci-service-audit-5f775dd975-brfdc
ci-service-datalake-ingestion-85b5bdfd6d-2qbwr
service-foundation-ingest-767dfd5bfc-vxd5p

Note that Wildcard and Expression filtering works with text or lists but not with numerics, dates or booleans.

Advanced Text Filtering with Contextual Type-Ahead Suggestions

Filtering in widget queries is *contextual*; when you select a filter value or values for a field, the other filters for that query will show values relevant to that filter.

For example, when setting a filter for a specific object *Name*, the field to filter for *Model* will only show values relevant to that object *Name*.

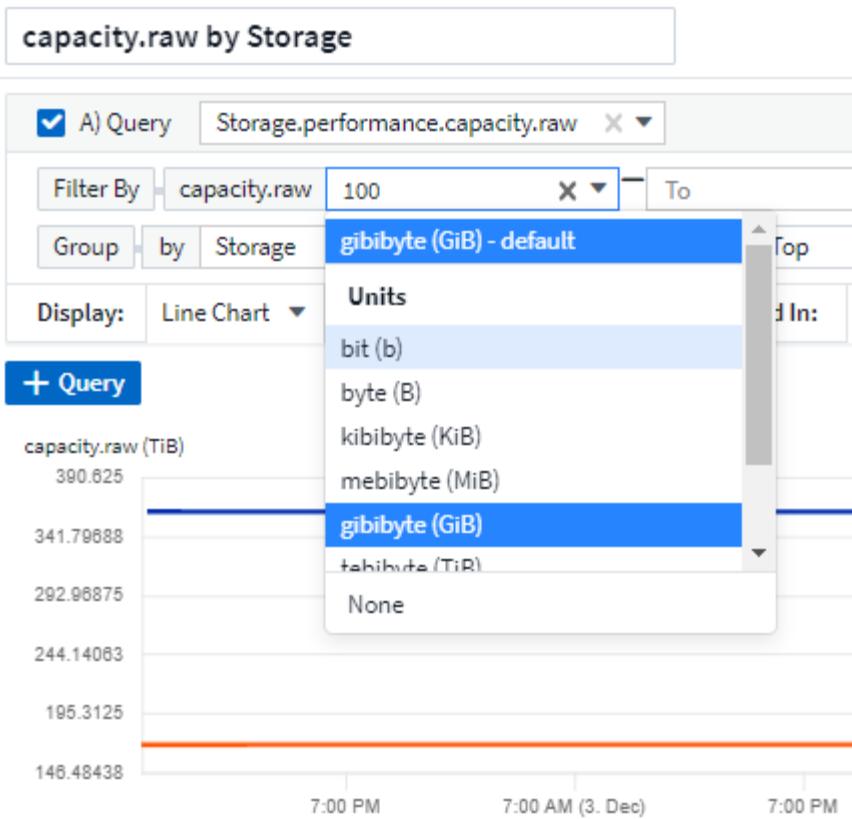
Contextual filtering also applies to dashboard page variables (text-type attributes or annotations only). When you select a filer value for one variable, any other variables using related objects will only show possible filter values based on the context of those related variables.

Note that only Text filters will show contextual type-ahead suggestions. Date, Enum (list), etc. will not show type-ahead suggestions. That said, you *can* set a filter on an Enum (i.e. list) field and have other text fields be filtered in context. For example, selecting a value in an Enum field like Data Center, then other filters will show only the models/names in that data center), but not vice-versa.

The selected time range will also provide context for the data shown in filters.

Choosing the filter units

As you type a value in a filter field, you can select the units in which to display the values on the chart. For example, you can filter on raw capacity and choose to display in the default GiB, or select another format such as TiB. This is useful if you have a number of charts on your dashboard showing values in TiB and you want all your charts to show consistent values.



Additional Filtering Refinements

The following can be used to further refine your filters.

- An asterisk enables you to search for everything. For example,

```
vol*rhel
```

displays all resources that start with "vol" and end with "rhel".

- The question mark enables you to search for a specific number of characters. For example,

```
BOS-PRD??-S12
```

displays *BOS-PRD12-S12*, *BOS-PRD13-S12*, and so on.

- The OR operator enables you to specify multiple entities. For example,

```
FAS2240 OR CX600 OR FAS3270
```

finds multiple storage models.

- The NOT operator allows you to exclude text from the search results. For example,

NOT EMC*

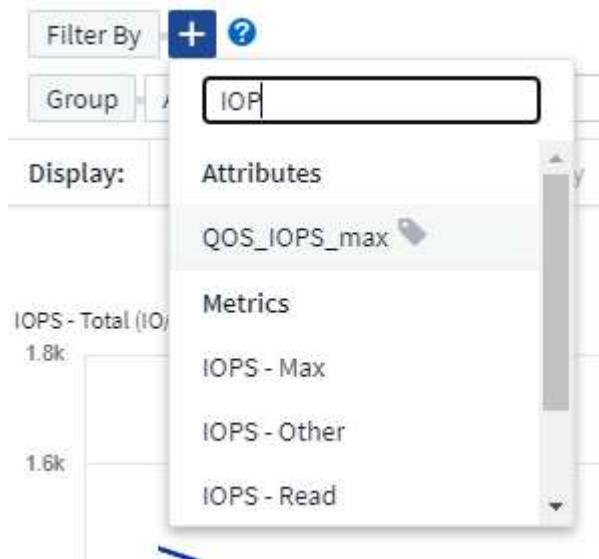
finds everything that does not start with "EMC". You can use

NOT *

to display fields that contain no value.

Identifying objects returned by queries and filters

The objects returned by queries and filters look similar to those shown in the following illustration. Objects with 'tags' assigned to them are annotations while the objects without tags are performance counters or object attributes.



Grouping and Aggregation

Grouping (Rolling Up)

Data displayed in a widget is grouped (sometimes called rolled-up) from the underlying data points collected during acquisition. For example, if you have a line chart widget showing Storage IOPS over time, you might want to see a separate line for each of your data centers, for a quick comparison. You can choose to group this data in one of several ways:

- **Average:** displays each line as the *average* of the underlying data.
- **Maximum:** displays each line as the *maximum* of the underlying data.
- **Minimum:** displays each line as the *minimum* of the underlying data.
- **Sum:** displays each line as the *sum* of the underlying data.
- **Count:** displays a *count* of objects that have reported data within the specified time frame. You can choose the *Entire Time Window* as determined by the dashboard time range (or the widget time range, if set to override the dashboard time), or a *Custom Time Window* that you select.

Steps

To set the grouping method, do the following.

1. In your widget's query, choose an asset type and metric (for example, *Storage*) and metric (such as *Performance IOPS Total*).
2. For **Group**, choose a roll up method (such as *Average*) and select the attributes or metrics by which to roll up the data (for example, *Data Center*).

The widget updates automatically and shows data for each of your data centers.

You can also choose to group *all* of the underlying data into the chart or table. In this case, you will get a single line for each query in the widget, which will show the average, min, max, sum, or count of the chosen metric or metrics for all of the underlying assets.

Clicking the legend for any widget whose data is grouped by "All" opens a query page showing the results of the first query used in the widget.

If you have set a filter for the query, the data is grouped based on the filtered data.

Note that when you choose to group a widget by any field (for example, *Model*), you will still need to Filter by that field in order to properly display the data for that field on the chart or table.

Aggregating data

You can further align your time-series charts (line, area, etc.) by aggregating data points into minute, hour, or day buckets before that data is subsequently rolled up by attribute (if chosen). You can choose to aggregate data points according to their *Average*, *Maximum*, *Minimum*, *Sum*, or *Count*.

A small interval combined with a long time range may result in an "Aggregation interval resulted in too many data points." warning. You might see this if you have a small interval and increase the dashboard time frame to 7 days. In this case, Insight will temporarily increase the aggregation interval until you select a smaller time frame.

You can also aggregate data in the bar chart widget and single-value widget.

Most asset counters aggregate to *Average* by default. Some counters aggregate to *Max*, *Min*, or *Sum* by default. For example, port errors aggregate to *Sum* by default, where storage IOPS aggregate to *Average*.

Showing Top/Bottom Results

In a chart widget, you can show either the **Top** or **Bottom** results for rolled up data, and choose the number of results shown from the drop-down list provided. In a table widget, you can sort by any column.

Chart widget top/bottom

In a chart widget, when you choose to rollup data by a specific attribute, you have the option of viewing either the top N or bottom N results. Note that you cannot choose the top or bottom results when you choose to rollup by *all* attributes.

You can choose which results to display by choosing either **Top** or **Bottom** in the query's **Show** field, and selecting a value from the list provided.

Table widget show entries

In a table widget, you can select the number of results shown in the table results. You are not given the option to choose top or bottom results because the table allows you to sort ascending or descending by any column on demand.

You can choose the number of results to show in the table on the dashboard by selecting a value from the query's **Show entries** field.

Grouping in Table Widget

Data in a table widget can be grouped by any available attribute, allowing you to see an overview of your data, and to drill-down into it for more detail. Metrics in the table are rolled up for easy viewing in each collapsed row.

Table widgets allow you to group your data based on the attributes you set. For example, you might want your table to show total storage IOPS grouped by the data centers in which those storages live. Or you might want to display a table of virtual machines grouped according to the hypervisor that hosts them. From the list, you can expand each group to view the assets in that group.

Grouping is only available in the Table widget type.

Grouping example (with rollup explained)

Table widgets allow you to group data for easier display.

In this example, we will create a table widget showing all VMs grouped by Data Center.

Steps

1. Create or open a dashboard, and add a **Table** widget.
2. Select *Virtual Machine* as the asset type for this widget.
3. Click on the Column Selector and choose *Hypervisor name* and *IOPS - Total*.

Those columns are now displayed in the table.

4. Let's disregard any VM's with no IOPS, and include only VMs that have total IOPS greater than 1. Click the **Filter by [+]** button and select *IOPS - Total*. Click on *Any*, and in the **from** field, type **1**. Leave the **to** field empty. Hit Enter or click off the filter field to apply the filter.

The table now shows all VMs with Total IOPS greater than or equal to 1. Notice that there is no grouping in the table. All VMs are shown.

5. Click the **Group by [+]** button.

You can group by any attribute or annotation shown. Choose *All* to display all VMs in a single group.

Any column header for a performance metric displays a "three dot" menu containing a **Roll up** option. The default roll up method is *Average*. This means that the number shown for the group is the average of all the Total IOPS reported for each VM inside the group. You can choose to roll this column up by *Average*, *Sum*, *Minimum* or *Maximum*. Any column that you display that contains performance metrics can be rolled up individually.



6. Click **All** and select *Hypervisor name*.

The VM list is now grouped by Hypervisor. You can expand each hypervisor to view the VMs hosted by it.

7. Click **Save** to save the table to the dashboard. You can resize or move the widget as desired.
8. Click **Save** to save the dashboard.

Performance data roll up

If you include a column for performance data (for example, *IOPS - Total*) in a table widget, when you choose to group the data you can then choose a roll up method for that column. The default roll up method is to display the average (avg) of the underlying data in the group row. You can also choose to display the sum, minimum, or maximum of the data.

Dashboard time range selector

You can select the time range for your dashboard data. Only data relevant to the selected time range will be displayed in widgets on the dashboard. You can select from the following time ranges:

- Last 15 Minutes
- Last 30 Minutes
- Last 60 Minutes
- Last 2 Hours
- Last 3 Hours (this is the default)
- Last 6 Hours
- Last 12 Hours
- Last 24 Hours
- Last 2 Days
- Last 3 Days
- Last 7 Days

- Last 30 Days
- Custom time range

The Custom time range allows you to select up to 31 consecutive days. You can also set the Start Time and End Time of day for this range. The default Start Time is 12:00 AM on the first day selected and the default End Time is 11:59 PM on the last day selected. Clicking **Apply** will apply the custom time range to the dashboard.

Overriding Dashboard Time in Individual widgets

You can override the main dashboard time range setting in individual widgets. These widgets will display data based on their set time frame, not the dashboard time frame.

To override the dashboard time and force a widget to use its own time frame, in the widget's edit mode set the **Override dashboard time** to **On** (check the box), and select a time range for the widget. **Save** the widget to the dashboard.

The widget will display its data according to the time frame set for it, regardless of the time frame you select on the dashboard itself.

The time frame you set for one widget will not affect any other widgets on the dashboard.

Primary and Secondary Axis

Different metrics use different units of measurements for the data they report in a chart. For example, when looking at IOPS, the unit of measurement is the number of I/O operations per second of time (IO/s), while Latency is purely a measure of time (milliseconds, microseconds, seconds, etc.). When charting both metrics on a single line chart using a single set of values for the Y-Axis, the latency numbers (typically a handful of milliseconds) are charted on the same scale with the IOPS (typically numbering in the thousands), and the latency line gets lost at that scale.

But it is possible to chart both sets of data on a single meaningful graph, by setting one unit of measurement on the primary (left-side) Y-axis, and the other unit of measurement on the secondary (right-side) Y-axis. Each metric is charted at its own scale.

Steps

This example illustrates the concept of Primary and Secondary axes in a chart widget.

1. Create or open a dashboard. Add a line chart, spline chart, area chart or stacked area chart widget to the dashboard.
2. Select an asset type (for example *Storage*) and choose *IOPS - Total* for your first metric. Set any filters you like, and choose a roll-up method if desired.

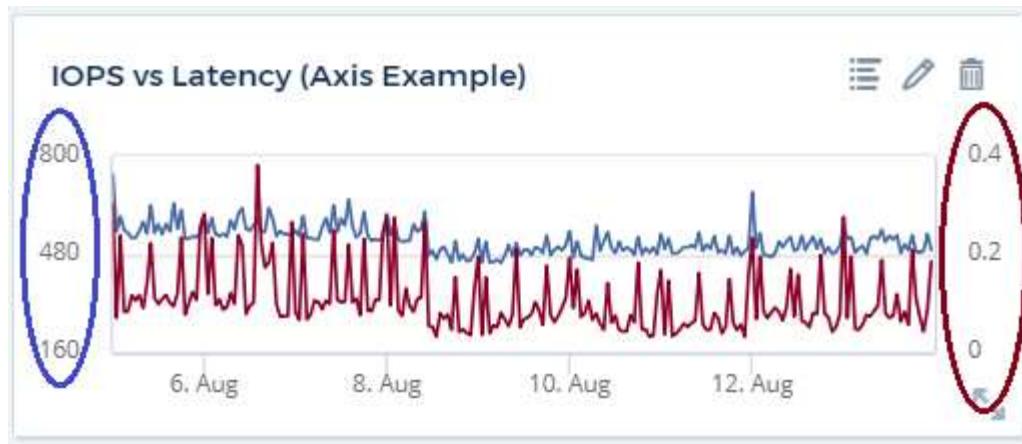
The IOPS line is displayed on the chart, with its scale shown on the left.

3. Click **[+Query]** to add a second line to the chart. For this line, choose *Latency - Total* for the metric.

Notice that the line is displayed flat at the bottom of the chart. This is because it is being drawn *at the same scale* as the IOPS line.

4. In the Latency query, select **Y-Axis: Secondary**.

The Latency line is now drawn at its own scale, which is displayed on the right side of the chart.



Expressions in widgets

In a dashboard, any time series widget (line, spline, area, stacked area), Single-Value, or Gauge Widget allows you to build expressions from metrics you choose, and show the result of those expressions in a single graph. The following examples use expressions to solve specific problems. In the first example, we want to show Read IOPS as a percentage of Total IOPS for all storage assets in our environment. The second example gives visibility into the "system" or "overhead" IOPS that occur in your environment—those IOPS that are not directly from reading or writing data.

You can use variables in expressions (for example, `$Var1 * 100`)

Expressions Example: Read IOPS percentage

In this example, we want to show Read IOPS as a percentage of Total IOPS. You can think of this as the following formula:

$$\text{Read Percentage} = (\text{Read IOPS} / \text{Total IOPS}) \times 100$$

This data can be shown in a line graph on your dashboard. To do this, follow these steps:

Steps

1. Create a new dashboard, or open an existing dashboard in edit mode.
2. Add a widget to the dashboard. Choose **Area chart**.

The widget opens in edit mode. By default, a query is displayed showing *IOPS - Total* for *Storage* assets. If desired, select a different asset type.

3. Click the **Convert to Expression** link on the right.

The current query is converted to Expression mode. Notice that you cannot change the asset type while in Expression mode. While you are in Expression mode, the link changes to **Revert to Query**. Click this if you wish to switch back to Query mode at any time. Be aware that switching between modes will reset fields to their defaults.

For now, stay in Expression mode.

4. The **IOPS - Total** metric is now in the alphabetic variable field "**a**". In the "**b**" variable field, click **Select** and choose **IOPS - Read**.

You can add up to a total of five alphabetic variables for your expression by clicking the + button following the variable fields. For our Read Percentage example, we only need Total IOPS ("a") and Read IOPS ("b").

5. In the **Expression** field, you use the letters corresponding to each variable to build your expression. We know that Read Percentage = (Read IOPS / Total IOPS) x 100, so we would write this expression as:

```
(b / a) * 100
```

6. The **Label** field identifies the expression. Change the label to "Read Percentage", or something equally meaningful for you.
7. Change the **Units** field to "%" or "Percent".

The chart displays the IOPS Read percentage over time for the chosen storage devices. If desired, you can set a filter, or choose a different rollup method. Be aware that if you select Sum as the rollup method, all percentage values are added together, which potentially may go higher than 100%.

8. Click **Save** to save the chart to your dashboard.

You can also use expressions in Line chart, Spline chart, or Stacked Area chart widgets.

Expressions example: "System" I/O

Example 2: Among the metrics collected from data sources are read, write, and total IOPS. However, the total number of IOPS reported by a data source sometimes includes "system" IOPS, which are those IO operations that are not a direct part of data reading or writing. This system I/O can also be thought of as "overhead" I/O, necessary for proper system operation but not directly related to data operations.

To show these system I/Os, you can subtract read and write IOPS from the total IOPS reported from acquisition. The formula might look like this:

```
System IOPS = Total IOPS - (Read IOPS + Write IOPS)
```

This data can then be shown in a line graph on your dashboard. To do this, follow these steps:

Steps

1. Create a new dashboard, or open an existing dashboard in edit mode.
2. Add a widget to the dashboard. Choose **Line chart**.

The widget opens in edit mode. By default, a query is displayed showing *IOPS - Total* for *Storage assets*. If desired, select a different asset type.

3. In the **Roll Up** field, choose *Sum by All*.

The Chart displays a line showing the sum of total IOPS.

4. Click the *Duplicate this Query* icon  to create a copy of the query.

A duplicate of the query is added below the original.

5. In the second query, click the **Convert to Expression** button.

The current query is converted to Expression mode. Click **Revert to Query** if you wish to switch back to Query mode at any time. Be aware that switching between modes will reset fields to their defaults.

For now, stay in Expression mode.

6. The *IOPS - Total* metric is now in the alphabetic variable field "a". Click on *IOPS - Total* and change it to *IOPS - Read*.

7. In the "b" variable field, click **Select** and choose *IOPS - Write*.

8. In the **Expression** field, you use the letters corresponding to each variable to build your expression. We would write our expression simply as:

```
a + b
```

In the Display section, choose **Area chart** for this expression.

9. The **Label** field identifies the expression. Change the label to "System IOPS", or something equally meaningful for you.

The chart displays the total IOPS as a line chart, with an area chart showing the combination of read and write IOPS below that. The gap between the two shows the IOPS that are not directly related to data read or write operations. These are your "system" IOPS.

10. Click **Save** to save the chart to your dashboard.

To use a variable in an expression, simply type the variable name, for example, `$var1 * 100`. Only numeric variables can be used in expressions.

Variables

Variables allow you to change the data displayed in some or all widgets on a dashboard at once. By setting one or more widgets to use a common variable, changes made in one place cause the data displayed in each widget to update automatically.

Dashboard variables come in several types, can be used across different fields, and must follow rules for naming. These concepts are explained here.

Variable types

A variable can be one the following types:

- **Attribute:** Use an object's attributes or metrics to filter
- **Annotation:** Use a pre-defined [Annotation](#) to filter widget data.
- **Text:** An alphanumeric string.
- **Numerical:** A number value. Use by itself, or as a "from" or "to" value, depending on your widget field.
- **Boolean:** Use for fields with values of True/False, Yes/No, etc. For the boolean variable, the choices are Yes, No, None, Any.
- **Date:** A date value. Use as a "from" or "to" value, depending on your widget's configuration.



Attribute variables

Selecting an Attribute type variable allows you to filter for widget data containing the specified attribute value or values. The example below shows a line widget displaying free memory trends for Agent nodes. We have created a variable for Agent Node IPs, currently set to show all IPs:



But if you temporarily want to see only nodes on individual subnets in your environment, you can set or change the variable to a specific Agent Node IP or IPs. Here we are viewing only the nodes on the "123" subnet:



You can also set a variable to filter on *all* objects with a particular attribute regardless of object type, for example objects with an attribute of "vendor", by specifying `*.vendor` in the variable field. You do not need to type the `"*."`; Cloud Insights will supply this if you select the wildcard option.

The screenshot shows a dropdown menu titled "Attribute" with the search term "vendor" entered. The results list includes "Objects containing 'vendor'" and several specific object types followed by ".vendor": "Disk.vendor", "GenericDevice.vendor", "Storage.vendor", "StoragePool.vendorTier", "Switch.vendor", "Tape.vendor", "InternalVolume.storage.vendor", and "netapp_ontap.disk_constituent.vendor".

When you drop-down the list of choices for the variable value, the results are filtered so show only the available vendors based on the objects on your dashboard.



If you edit a widget on your dashboard where the attribute filter is relevant (meaning, the widget's objects contain any `*.vendor` attribute), it shows you that the attribute filter is automatically applied.

A screenshot of a dashboard configuration screen for a "Count of Storages" widget. The query is set to "Storage.performance.iops.total". In the "Filter By" section, there is a dropdown for "name" set to "All", and another dropdown for "vendor" set to "NETAPP". A tooltip states "This is an automatically applied filter from dashboard variables". Below the filters, there are sections for "Formatting" (with options for value comparison, warning/critical thresholds, and color coding), "Description" (e.g., Total IOPS), "Calculation" (set to "A"), and "Decimal Places" (set to 0). A "Reset Defaults" button is also present. At the bottom left is a blue "+ Query" button.

14

Applying variables is as easy as changing the attribute data of your choice.

Annotation variables

Choosing an Annotation variable allows you to filter for objects associated with that annotation, for example, those belonging to the same Data Center.



Text, Number, Date, or Boolean variable

You can create generic variables that are not associated with a particular attribute by selecting a variable type of *Text*, *Number*, *Boolean*, or *Date*. Once the variable has been created, you can select it in a widget filter field. When setting a filter in a widget, in addition to specific values that you can select for the filter, any variables that have been created for the dashboard are displayed in the list—these are grouped under the "Variables" section in the drop-down and have names starting with "\$". Choosing a variable in this filter will allow you to search for values that you enter in the variable field on the dashboard itself. Any widgets using that variable in a filter will be updated dynamically.

The screenshot shows a table titled "Disk" with 324 items found. The table has a "Disk" column and a "Name" column. The "Name" column is currently filtered to show "All" items. A dropdown menu is open over the "Name" column, listing items starting with "0a.", such as "0a.16", "0a.17", "0a.18", etc. At the bottom of this dropdown menu, there is a section labeled "Variables" containing "\$agent_node_ip" and "\$var1". A "None" option is also available at the bottom.

Variable Filter Scope

When you add an Annotation or Attribute variable to your dashboard, the variable can be applied to *all* widgets on the dashboard, meaning that all widgets on your dashboard will display results filtered according to the

value you set in the variable.



Note that only Attribute and Annotation variables can be filtered automatically like this. Non-Annotation or -Attribute variables cannot be automatically filtered. Individual widgets must each be configured to use variables of these types.

To disable automatic filtering so that the variable only applies to the widgets where you have specifically set it, click the "Filter automatically" slider to disable it.

To set a variable in an individual widget, open the widget in edit mode and select the specific annotation or attribute in the *Filter By* field. With an Annotation variable, you can select one or more specific values, or select the Variable name (indicated by the leading "\$") to allow typing in the variable at the dashboard level. The same applies to Attribute variables. Only those widgets for which you set the variable will show the filtered results.

Filtering in variables is *contextual*; when you select a filter value or values for a variable, the other variables on your page will show only values relevant to that filter.

For example, when setting a variable filter to a specific storage *Model*, any variables set to filter for storage *Name* will only show values relevant to that Model.

To use a variable in an expression, simply type the variable name as part of the expression, for example, \$var1 * 100. Only Numeric variables can be used in expressions. You cannot use numeric Annotation or Attribute variables in expressions.

Filtering in variables is *contextual*; when you select a filter value or values for a variable, the other variables on your page will show only values relevant to that filter.

For example, when setting a variable filter to a specific storage *Model*, any variables set to filter for storage *Name* will only show values relevant to that Model.

Variable naming

Variables names:

- Must include only the letters a-z, the digits 0-9, period (.), underscore (_), and space ().
- Cannot be longer than 20 characters.
- Are case-sensitive: \$CityName and \$cityname are different variables.
- Cannot be the same as an existing variable name.
- Cannot be empty.

Formatting Gauge Widgets

The Solid and Bullet Gauge widgets allow you to set thresholds for *Warning* and/or *Critical* levels, providing clear representation of the data you specify.

Widget 12

Override Dashboard Time X

✓ A) Query Storage.performance.iops.total X

Filter By +

Group Avg Time aggregate by Avg Less Options

Formatting: If value is > Warning 500 IO/s and/or Critical 1000 IO/s Showing In Range as green

Description IOPS - Total	Calculation A	Min Value Optional	Max Value 1200
--------------------------	---------------	--------------------	----------------

Display: Bullet Gauge Decimal Places: 2 Color: Units Displayed In: Auto Format

904.21 IO/s
IOPS - Total ⚠

Cancel Save

To set formatting for these widgets, follow these steps:

1. Choose whether you want to highlight values greater than (>) or less than (<) your thresholds. In this example, we will highlight values greater than (>) the threshold levels.
2. Choose a value for the "Warning" threshold. When the widget displays values greater than this level, it displays the gauge in orange.
3. Choose a value for the "Critical" threshold. Values greater than this level will cause the gauge to display in red.

You can optionally choose a minimum and maximum value for the gauge. Values below minimum will not display the gauge. Values above maximum will display a full gauge. If you do not choose minimum or maximum values, the widget selects optimal min and max based on the widget's value.





Formatting Single-Value Widget

In the Single-Value widget, in addition to setting Warning (orange) and Critical (red) thresholds, you can choose to have "In Range" values (those below Warning level) shown with either green or white background.



Clicking the link in either a single-value widget or a gauge widget will display a query page corresponding to the first query in the widget.

Formatting Table Widgets

Like single-value and gauge widgets, you can set conditional formatting in table widgets, allowing you to highlight data with colors and/or special icons.

Conditional Formatting allows you to set and highlight Warning-level and Critical-level thresholds in table widgets, bringing instant visibility to outliers and exceptional data points.

14 items found in 1 group		
Table Row Grouping	Expanded Detail	Metrics & Attributes
<input type="checkbox"/> All	Storage Pool	capacityRatio.used (%)
<input type="checkbox"/> All (14)	--	95.15
--	rtp-sa-cl06-02:aggr_data1_rtp_sa_cl06_02	0.79
--	rtp-sa-cl06-01:aggr_data1_rtp_sa_cl06_01	2.45
--	rtp-sa-cl06-02:aggro_rtp_sa_cl06_02_root	95.15
--	rtp-sa-cl06-01:aggro_rtp_sa_cl06_01_root	95.15
Formatting: <input checked="" type="checkbox"/> Show Expanded Details <input type="checkbox"/> Conditional Formatting <input type="checkbox"/> Background Color + Icon <input type="checkbox"/> Show <input checked="" type="checkbox"/> In Range as green		

Conditional formatting is set separately for each column in a table. For example, you can choose one set of thresholds for a capacity column, and another set for a throughput column.

If you change the Unit Display for a column, the conditional formatting remains and reflects the change in values. The images below show the same conditional formatting even though the display unit is different.

The image consists of two vertically stacked screenshots from a Cloud Insights dashboard configuration interface.

Top Screenshot: This shows the configuration for the "capacity.used (GiB)" column. The values listed are 40,754.06, 10,313.56, 9,544.84, 8,438.99, and 6,671.72. The "throughput.total (MiB/s)" column is shown on the right with its own configuration panel. The "Conditional Formatting" section is expanded, showing a warning threshold of 8000 GiB and a critical threshold of 10000 GiB. A "Unit Display" section is also present.

capacity.used (GiB)
40,754.06
10,313.56
9,544.84
8,438.99
6,671.72

Bottom Screenshot: This shows the configuration for the "capacity.used (TiB)" column. The values listed are 39.80, 10.07, 9.32, 8.24, and 6.52. The "throughput.total (MiB/s)" column is shown on the right with its own configuration panel. The "Unit Display" section is expanded, showing a dropdown menu for "Base Unit" with options including "gibibyte (GiB)", "tebibyte (TiB)" (which is selected), "gigabyte (GB)", "terabyte (TB)", "pebibyte (PiB)", and "petabyte (PB)". A "Conditional Formatting" section is also present.

capacity.used (TiB)
39.80
10.07
9.32
8.24
6.52

You can choose whether to display condition formatting as color, icons, or both.

Choosing the Unit for Displaying Data

Most widgets on a dashboard allow you to specify the Units in which to display values, for example *Megabytes*, *Thousands*, *Percentage*, *Milliseconds (ms)*, etc. In many cases, Cloud Insights knows the best format for the data being acquired. In cases where the best format is not known, you can set the format you want.

In the line chart example below, the data selected for the widget is known to be in *bytes* (the base IEC Data

unit: see the table below), so the Base Unit is automatically selected as 'byte (B)'. However, the data values are large enough to be presented as gibibytes (GiB), so Cloud Insights by default auto-formats the values as GiB. The Y-axis on the graph shows 'GiB' as the display unit, and all values are displayed in terms of that unit.



If you want to display the graph in a different unit, you can choose another format in which to display the values. Since the base unit in this example is *byte*, you can choose from among the supported "byte-based" formats: bit (b), byte (B), kibibyte (KiB), mebibyte (MiB), gibibyte (GiB). The Y-Axis label and values change according to the format you choose.



In cases where the base unit is not known, you can assign a unit from among the [available units](#), or type in your own. Once you assign a base unit, you can then select to display the data in one of the appropriate supported formats.



To clear out your settings and start again, click on **Reset Defaults**.

A word about Auto-Format

Most metrics are reported by data collectors in the smallest unit, for example as a whole number such as 1,234,567,890 bytes. By default, Cloud Insights will automatically format the value for the most readable display. For example a data value of 1,234,567,890 bytes would be auto formatted to 1.23 *Gibabytes*. You can choose to display it in another format, such as *Mebibytes*. The value will display accordingly.



Cloud Insights uses American English number naming standards. American "billion" is equivalent to "thousand million".

Widgets with multiple queries

If you have a time-series widget (i.e. line, spline, area, stacked area) that has two queries where both are plotted on the primary Y-Axis, the base unit is not shown at the top of the Y-Axis. However, if your widget has a query on the primary Y-Axis and a query on the secondary Y-Axis, the base units for each are shown.



If your widget has three or more queries, base units are not shown on the Y-Axis.

Available Units

The following table shows all the available units by category.

Category	Units
----------	-------

Currency	cent dollar
Data(IEC)	bit byte kibibyte mebibyte gibibyte tebibyte pebibyte exbibyte
DataRate(IEC)	bit/sec byte/sec kibibyte/sec mebibyte/sec gibibyte/sec tebibyte/sec pebibyte/sec
Data(Metric)	kilobyte megabyte gigabyte terabyte petabyte exabyte
DataRate(Metric)	kilobyte/sec megabyte/sec gigabyte/sec terabyte/sec petabyte/sec exabyte/sec
IEC	kibi mebi gibi tebi pebi exbi
Decimal	whole number thousand million billion trillion
Percentage	percentage
Time	nanosecond microsecond millisecond second minute hour

Temperature	celsius fahrenheit
Frequency	hertz kilohertz megahertz gigahertz
CPU	nanocores microcores millicores cores kilocores megacores gigacores teracores petacores exacores
Throughput	I/O ops/sec ops/sec requests/sec reads/sec writes/sec ops/min reads/min writes/min

TV Mode and Auto-Refresh

Data in widgets on Dashboards and Asset Landing Pages auto-refresh according a refresh interval determined by the Dashboard Time Range selected (or widget time range, if set to override the dashboard time). The refresh interval is based on whether the widget is time-series (line, spline, area, stacked area chart) or non-time-series (all other charts).

Dashboard Time Range	Time-Series Refresh Interval	Non-Time-Series Refresh Interval
Last 15 Minutes	10 Seconds	1 Minute
Last 30 Minutes	15 Seconds	1 Minute
Last 60 Minutes	15 Seconds	1 Minute
Last 2 Hours	30 Seconds	5 Minutes
Last 3 Hours	30 Seconds	5 Minutes
Last 6 Hours	1 Minute	5 Minutes
Last 12 Hours	5 Minutes	10 Minutes
Last 24 Hours	5 Minutes	10 Minutes
Last 2 Days	10 Minutes	10 Minutes
Last 3 Days	15 Minutes	15 Minutes
Last 7 Days	1 Hour	1 Hour

Last 30 Days	2 Hours	2 Hours
--------------	---------	---------

Each widget displays its auto-refresh interval in the upper-right corner of the widget.

Auto-refresh is not available for Custom dashboard time range.

When combined with **TV Mode**, auto-refresh allows for near-real-time display of data on a dashboard or asset page. TV Mode provides an uncluttered display; the navigation menu is hidden, providing more screen real estate for your data display, as is the Edit button. TV Mode ignores typical Cloud Insights timeouts, leaving the display live until logged out manually or automatically by authorization security protocols.



Because NetApp Cloud Central has its own user login timeout of 7 days, Cloud Insights must log out with that event as well. You can simply log in again and your dashboard will continue to display.

- To activate TV Mode, click the **TV Mode** button.
-



To disable TV Mode, click the **Exit** button in the upper left of the screen.

You can temporarily suspend auto-refresh by clicking the Pause button in the upper right corner. While paused, the dashboard time range field will display the paused data's active time range. Your data is still being acquired and updated while auto-refresh is paused. Click the Resume button to continue auto-refreshing of data.



Dashboard Groups

Grouping allows you to view and manage related dashboards. For example, you can have a dashboard group dedicated to the storage in your environment. Dashboard groups are managed on the **Dashboards > Show All Dashboards** page.

Dashboard Groups (3)

All Dashboards (60)	+
My Dashboards (11)	◀
Storage Group (7)	⋮

Dashboards (7)

Name ↑
Dashboard - Storage Cost
Dashboard - Storage IO Detail
Dashboard - Storage Overview
Gauges Storage Performance
Storage Admin - Which nodes are in high demand?
Storage Admin - Which pools are in high demand?
Storage IOPs

Two groups are shown by default:

- **All Dashboards** lists all the dashboards that have been created, regardless of owner.
- **My Dashboards** lists only those dashboards created by the current user.

The number of dashboards contained in each group is shown next to the group name.

To create a new group, click the "+" **Create New Dashboard Group** button. Enter a name for the group and click **Create Group**. An empty group is created with that name.

To add dashboards to the group, click the *All Dashboards* group to show all dashboards in your environment, or click *My Dashboards* if you only want to see the dashboards you own, and do one of the following:

- To add a single dashboard, click the menu to the right of the dashboard and select *Add to Group*.
- To add multiple dashboards to a group, select them by clicking the checkbox next to each dashboard, then click the **Bulk Actions** button and select *Add to Group*.

Remove dashboards from the current group in the same manner by selecting *Remove From Group*. You can not remove dashboards from the *All Dashboards* or *My Dashboards* group.

 Removing a dashboard from a group does not delete the dashboard from Cloud Insights. To completely remove a dashboard, select the dashboard and click *Delete*. This removes it from any groups to which it belonged and it is no longer available to any user.

Pin your Favorite Dashboards

You can further manage your dashboards by pinning favorite ones to the top of your dashboard list. To pin a dashboard, simply click the thumbtack button displayed when you hover over a dashboard in any list.

Dashboard pin/unpin is an individual user preference and independent of the group (or groups) to which the dashboard belongs.

Dashboards (7)

<input type="checkbox"/>	Name ↑
	Dashboard - Storage Overview
	Storage Admin - Which nodes are in high demand?
	Storage IOPs
	Dashboard - Storage Cost
	Dashboard - Storage IO Detail
	Gauges Storage Performance
	Storage Admin - Which pools are in high demand?

Dark Theme

You can choose to display Cloud Insights using either a light theme (the default), which displays most screens using a light background with dark text, or a dark theme which displays most screens using a dark background with light text.

To switch between light and dark themes, click the username button in the upper right corner of the screen and choose the desired theme.



Dark Theme Dashboard view:



Light Theme Dashboard view:



Some screen areas, such as certain widget charts, still show light backgrounds even while viewed in dark theme.

Line Chart interpolation

Different data collectors often poll their data at different intervals. For example, data collector A may poll every 15 minutes while data collector B polls every five minutes. When a line chart widget (also spline, area, and stacked area charts) is aggregating this data from multiple data collectors into a single line (for example, when the widget is grouping by "all"), and refreshing the line every five minutes, data from collector B may be shown accurately while data from collector A may have gaps, thus affecting the aggregate until collector A polls again.

To alleviate this, Cloud Insights interpolates data when aggregating, using the surrounding data points to take a "best guess" at data until data collectors poll again. You can always view each data collector's object data individually by adjusting the widget's grouping.

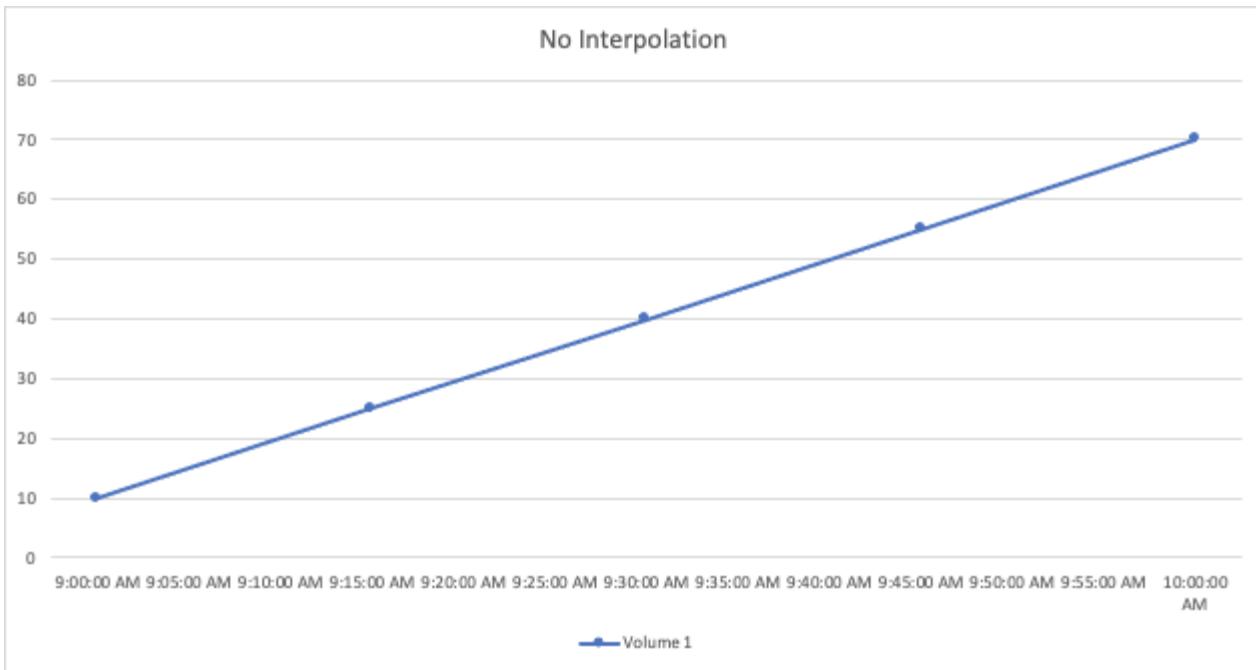
Interpolation Methods

When creating or modifying a line chart (or spline, area, or stacked area chart), you can set the interpolation method to one of three types. In the "Group by" section, choose the desired Interpolation.

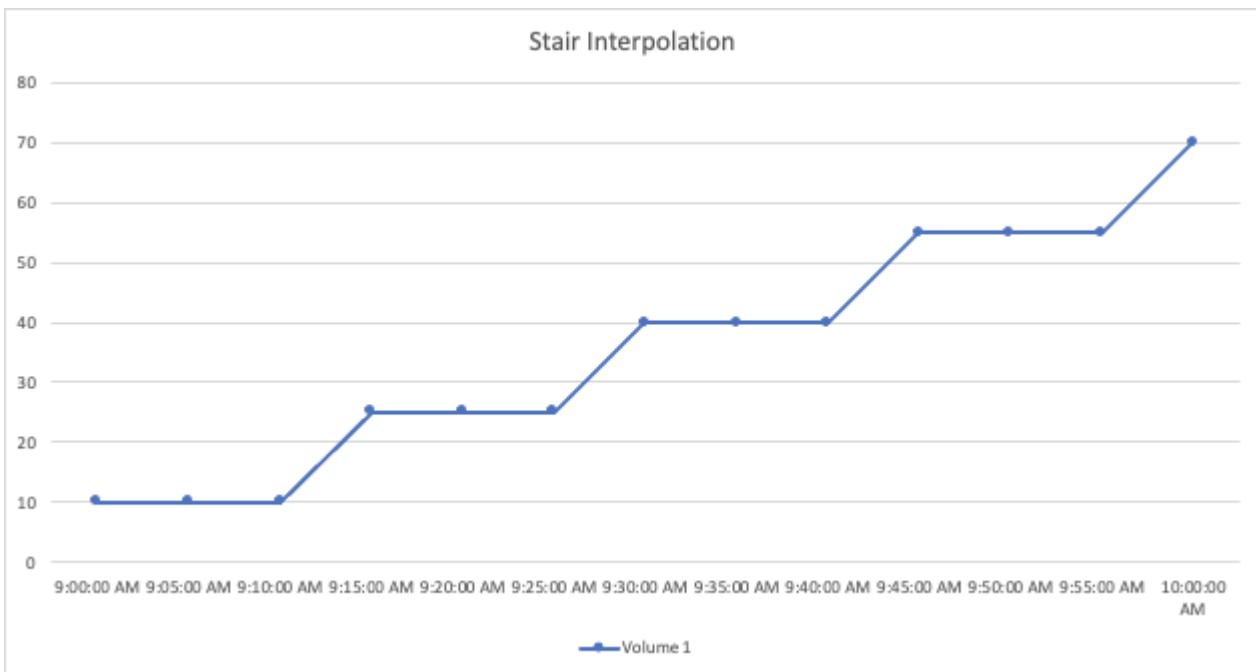
The screenshot shows the "Interpolation" dropdown menu in the Cloud Insights interface. The options available are:

- None
- Linear
- Stair

- **None:** Do nothing, i.e. do not generate points in between.



- **Stair:** A point is generated from the value of previous point. In a straight line, this would display as a typical "stair" layout.



- **Linear:** a point is generated as the value in between connecting the two points. Generates a line that looks like the line connecting the two points, but with additional (interpolated) data points.



Sample Dashboards

Dashboard Example: Virtual Machine Performance

There are many challenges facing IT operations today. Administrators are being asked to do more with less, and having full visibility into your dynamic data centers is a must. In this example, we will show you how to create a dashboard with widgets that give you operational insights into the virtual machine (VM) performance in your environment. By following this example, and creating widgets to target your own specific needs, you can do things like visualizing backend storage performance compared to frontend virtual machine performance, or viewing VM latency versus I/O demand.

About this task

Here we will create a Virtual Machine Performance dashboard containing the following:

- a table listing VM names and performance data
- a chart comparing VM Latency to Storage Latency
- a chart showing Read, Write and Total IOPS for VMs
- a chart showing Max Throughput for your VMs

This is just a basic example. You can customize your dashboard to highlight and compare any performance data you choose, in order to target for your own operational best practices.

Steps

1. Log in to Insight as a user with administrative permissions.
2. From the **Dashboards** menu, select **[+New dashboard]**.

The **New dashboard** page opens.

3. At the top of the page, enter a unique name for the dashboard, for example "VM Performance by Application".
4. Click **Save** to save the dashboard with the new name.
5. Let's start adding our widgets. If necessary, click the **Edit** icon to enable Edit mode.
6. Click the **Add Widget** icon and select **Table** to add a new table widget to the dashboard.

The Edit Widget dialog opens. The default data displayed is for all storages in your environment.

Table Widget ↻ 10m

1,746 items found in 71 groups

Hypervisor Name ↑	Virtual Machine	Capacity - Total (GB)	IOPS - Total (IO/s)	Latency - Total (ms)
[+] 10.197.143.53 (9)	--	1,690.58	1.80	12.04
[+] 10.197.143.54 (7)	--	1,707.60	4.62	12.69
[+] 10.197.143.57 (11)	--	1,509.94	1.14	1.15
[+] 10.197.143.58 (10)	--	1,818.34	5.83	2.57
[+] AzureComputeDefaultAvailabilitySet (363)	--	N/A	N/A	N/A
[+] anandh9162020113920-rg-avset.anandh9162020	--	N/A	N/A	N/A
[+] anandh916202013287-rg-avset.anandh9162020	--	N/A	N/A	N/A
[+] anandh91720201288-rg-avset.anandh91720201	--	N/A	N/A	N/A
[+] anjalivlngrun48-rg-avset.anjalivlngrun48-rg-398	--	N/A	N/A	N/A
[+] anjalivlngrun50-rg-avset.anjalivlngrun50-rg-398	--	N/A	N/A	N/A
[+] batutiscanaryHA97a-rg-avset.batutiscanaryha97	--	N/A	N/A	N/A
[+] batutiscanaryHA97b-rg-avset.batutiscanaryha97	--	N/A	N/A	N/A

1. We can customize this widget. In the Name field at the top, delete "Widget 1" and enter "Virtual Machine Performance table".
2. Click the asset type drop-down and change *Storage* to *Virtual Machine*.

The table data changes to show all virtual machines in your environment.

3. Let's add a few columns to the table. Click the Gear icon on the right and select *Hypervisor name*, *IOPS - Total*, and *Latency - Total*. You can also try typing the name into the search to quickly display the desired field.

These columns are now displayed in the table. You can sort the table by any of these columns. Note that the columns are displayed in the order in which they were added to the widget.

4. For this exercise we will exclude VMs that are not actively in use, so let's filter out anything with less than 10 total IOPS. Click the **[+]** button next to **Filter by** and select *IOPS - Total*. Click on **Any** and enter "10" in the **from** field. Leave the **to** field empty. Click outside the filter field or press Enter to set the filter.

The table now shows only VMs with 10 or more total IOPS.

5. We can further collapse the table by grouping results. Click the **[+]** button next to **Group by** and select a field to group by, such as *Application* or *Hypervisor name*. Grouping is automatically applied.

The table rows are now grouped according to your setting. You can expand and collapse the groups as needed. Grouped rows show rolled up data for each of the columns. Some columns allow you to choose the roll up method for that column.

Virtual Machine Performance Table

Override dashboard time Last 24 hours

Virtual Machine

Filter by: IOPS - Total (IO/s) >= 10 Group by Hypervisor name

181 items found in 4 groups

Hypervisor name ↓	Name	Hypervisor name	IOPS - Total (IO/s)	Latency - Total (ms)
<input type="button" value="+"/> us-east-1d (62)		us-east-1d	1.94	
<input type="button" value="+"/> us-east-1c (80)		us-east-1c	0.80	
<input type="button" value="+"/> us-east-1b (1)	TBDemoEnv	us-east-1b	32.66	0.70
<input type="button" value="+"/> us-east-1a (38)		us-east-1a	121.22	0.81

- When you have customized the table widget to your satisfaction, click the **[Save]** button.

The table widget is saved to the dashboard.

You can resize the widget on the dashboard by dragging the lower-right corner. Make the widget wider to show all the columns clearly. Click **Save** to save the current dashboard.

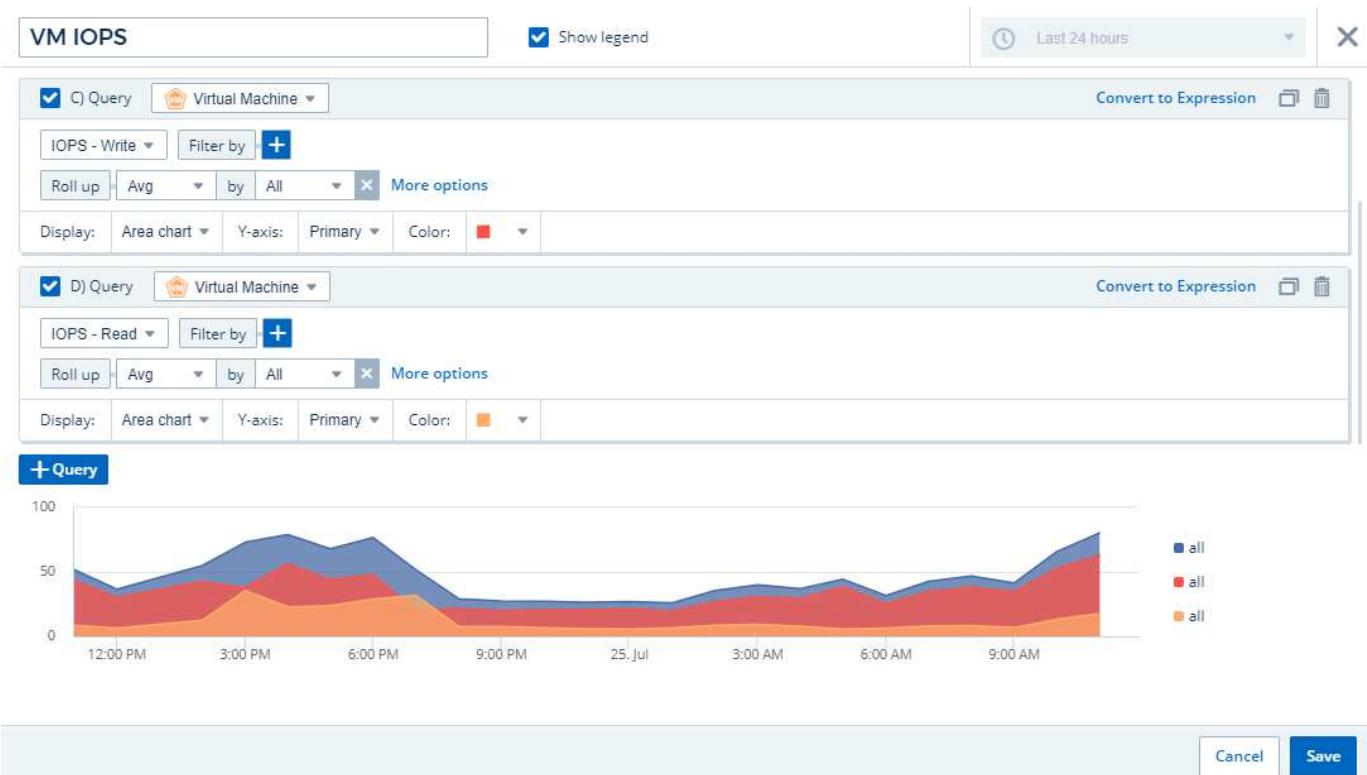
Next we will add some charts to show our VM Performance. Let's create a line chart comparing VM latency with VMDK latency.

- If necessary, click the **Edit** icon on the dashboard to enable Edit mode.
- Click the **[Add widget]** icon and select *Line Chart* to add a new line chart widget to the dashboard.
- The **Edit Widget** dialog opens. Name this widget "VM / VMDK Max Latency"
- Select **Virtual Machine** and choose *Latency - Max*. Set any filters you wish, or leave **Filter by** empty. For **Roll up**, choose *Sum by All*. Display this data as a *Line Chart*, and leave **Y-Axis** as *Primary*.
- Click the **[+Query]** button to add a second data line. For this line, select **VMDK** and *Latency - Max*. Set any filters you wish, or leave **Filter by** empty. For **Roll up**, choose *Sum by All*. Display this data as a *Line Chart*, and leave **Y-Axis** as *Primary*.
- Click **[Save]** to add this widget to the dashboard.



Next we will add a chart showing VM Read, Write and Total IOPS in a single chart.

1. Click the **[Add widget]** icon and select *Area Chart* to add a new area chart widget to the dashboard.
2. The Edit Widget dialog opens. Name this widget "VM IOPS"
3. Select **Virtual Machine** and choose *IOPS - Total*. Set any filters you wish, or leave **Filter by** empty. for **Roll up**, choose *Sum* by *All*. Display this data as an *Area Chart*, and leave *Y-Axis* as *Primary*.
4. Click the **[+Query]** button to add a second data line. For this line, select **Virtual Machine** and choose *IOPS - Read*.
5. Click the **[+Query]** button to add a third data line. For this line, select **Virtual Machine** and choose *IOPS - Write*.
6. Click **Show legend** to display a legend for this widget on the dashboard.



1. Click **[Save]** to add this widget to the dashboard.

Next we will add a chart showing VM Throughput for each Application associated with the VM. We will use the Roll Up feature for this.

1. Click the **[Add widget]** icon and select *Line Chart* to add a new line chart widget to the dashboard.
2. The Edit Widget dialog opens. Name this widget "VM Throughput by Application"
3. Select Virtual Machine and choose Throughput - Total. Set any filters you wish, or leave Filter by empty. For Roll up, choose "Max" and select by "Application" or "Name". Show the Top 10 applications. Display this data as a Line Chart, and leave Y-Axis as Primary.
4. Click **[Save]** to add this widget to the dashboard.

You can move widgets on the dashboard by holding down the mouse button anywhere in the top of the widget and dragging it to a new location.

You can resize widgets by dragging the lower-right corner.

Be sure to **[Save]** the dashboard after you make your changes.

Your final VM Performance Dashboard will look something like this:



Best Practices for Dashboards and Widgets

Tips and tricks to help you get the most out of the powerful features of dashboards and widgets.

Finding the Right Metric

Cloud Insights acquires counters and metrics using names that sometimes differ from data collector to data collector.

When searching for the right metric or counter for your dashboard widget, keep in mind that the metric you want could be under a different name from the one you are thinking of. While drop-down lists in Cloud Insights are usually alphabetical, sometimes a term may not show up in the list where you think it should. For example, terms like "raw capacity" and "used capacity" do not appear together in most lists.

Best practice: Use the search feature in fields such as Filter by or places like the column selector to find what you are looking for. For example, searching for "cap" will show all metrics with "capacity" in their names, no matter where they occur in the list. You can then easily select the metrics you want from that shorter list.

Here are a few alternative phrases you can try when searching for metrics:

When you want to find:	Try also searching for:
CPU	Processor
Capacity	Used capacity Raw capacity Provisioned capacity Storage pools capacity <other asset type> capacity Written capacity

Disk Speed	Lowest disk speed Least performing disk type
Host	Hypervisor Hosts
Hypervisor	Host Is hypervisor
Microcode	Firmware
Name	Alias Hypervisor name Storage name <other asset type> name Simple name Resource name Fabric Alias
Read / Write	Partial R/W Pending writes IOPS - Write Written capacity Latency - Read Cache utilization - read
Virtual Machine	VM Is virtual

This is not a comprehensive list. These are examples of possible search terms only.

Finding the Right Assets

The assets you can reference in widget filters and searches vary from asset type to asset type.

In dashboards and asset pages, the asset type around which you are building your widget determines the other asset type counters for which you can filter or add a column. Keep the following in mind when building your widget:

This asset type / counter:	Can be filtered for under these assets:
Virtual Machine	VMDK
Datastore(s)	Internal Volume VMDK Virtual Machine Volume
Hypervisor	Virtual Machine Is hypervisor Host
Host(s)	Internal Volume Volume Cluster Host Virtual Machine

Fabric	Port
--------	------

This is not a comprehensive list.

Best practice: If you are filtering for a particular asset type that does not appear in the list, try building your query around an alternate asset type.

Scatter Plot Example: Knowing your Axis

Changing the order of counters in a scatter plot widget changes the axes on which the data is displayed.

About this task

This example will create a scatter plot that will allow you to see under-performing VMs that have high latency compared to low IOPS.

Steps

1. Create or open a dashboard in edit mode and add a **Scatter Plot Chart** widget.
2. Select an asset type, for example, *Virtual Machine*.
3. Select the first counter you wish to plot. For this example, select *Latency - Total*.

Latency - Total is charted along the X-axis of the chart.

4. Select the second counter you wish to plot. For this example, select *IOPS - Total*.

IOPS - Total is charted along the Y-axis in the chart. VMs with higher latency display on the right side of the chart. Only the top 100 highest-latency VMs are displayed, because the **Top by X-axis** setting is current.



- Now reverse the order of the counters by setting the first counter to *IOPS - Total* and the second to *Latency - Total*.

Latency- Total is now charted along the Y-axis in the chart, and *IOPS - Total* along the X-axis. VMs with higher IOPS now display on the right side of the chart.

Note that because we haven't changed the **Top by X-Axis** setting, the widget now displays the top 100 highest-IOPS VMs, since this is what is currently plotted along the X-axis.



You can choose for the chart to display the Top N by X-axis, Top N by Y-axis, Bottom N by X-axis, or Bottom N by Y-axis. In our final example, the chart is displaying the Top 100 VMs that have the highest total IOPS. If we change it to **Top by Y-axis**, the chart will once again display the top 100 VMs that have the highest total latency.

Note that in a scatter plot chart, you can click on a point to drill down to the asset page for that resource.

Kubernetes Explorer

Kubernetes Cluster Overview

The Cloud Insights Kubernetes Explorer is a powerful tool for displaying the overall health and usage of your Kubernetes clusters and allows you to easily drill down into areas of investigation.

Clicking on **Dashboards > Kubernetes Explorer** opens the Kubernetes Cluster list page. This overview page contains table of the Kubernetes clusters in your environment.

Filter By [+](#) [?](#)

Clusters (2)

Name ↑	Overall Saturation (%)	CPU Saturation (%)	Memory Saturation (%)	Storage Saturation (%)	Nodes	Pods	Namespaces	Workloads
self	56	25	56	31	2	63	18	68
setoK3s	4	2	3	4	2	9	5	7

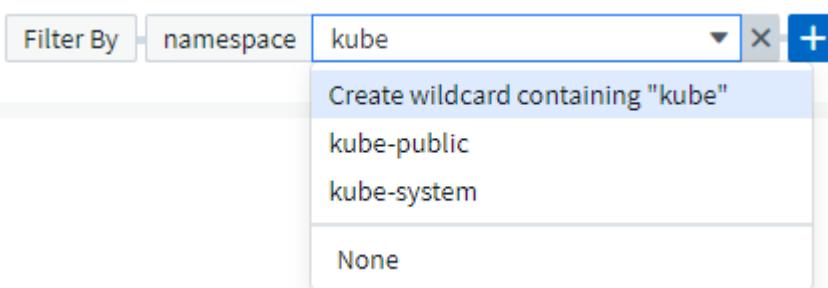
Cluster list

The cluster list displays the following information for each cluster in your environment:

- Cluster **Name**. Clicking on a cluster name will open the [detail page](#) for that cluster.
- **Saturation** percentages. Overall Saturation is the highest of CPU, Memory, or Storage Saturation.
- Number of **Nodes** in the cluster. Clicking this number will open the Node list page.
- Number of **Pods** in the cluster. Clicking this number will open the Pod list page.
- Number of **Namespaces** in the cluster. Clicking this number will open the Namespace list page.
- Number of **Workloads** in the cluster. Clicking this number will open the Workload list page.

Refining the Filter

When you are filtering, as you begin typing you are presented with the option to create a **wildcard filter** based on the current text. Selecting this option will return all results that match the wildcard expression. You can also create **expressions** using NOT or AND, or you can select the "None" option to filter for null values in the field.



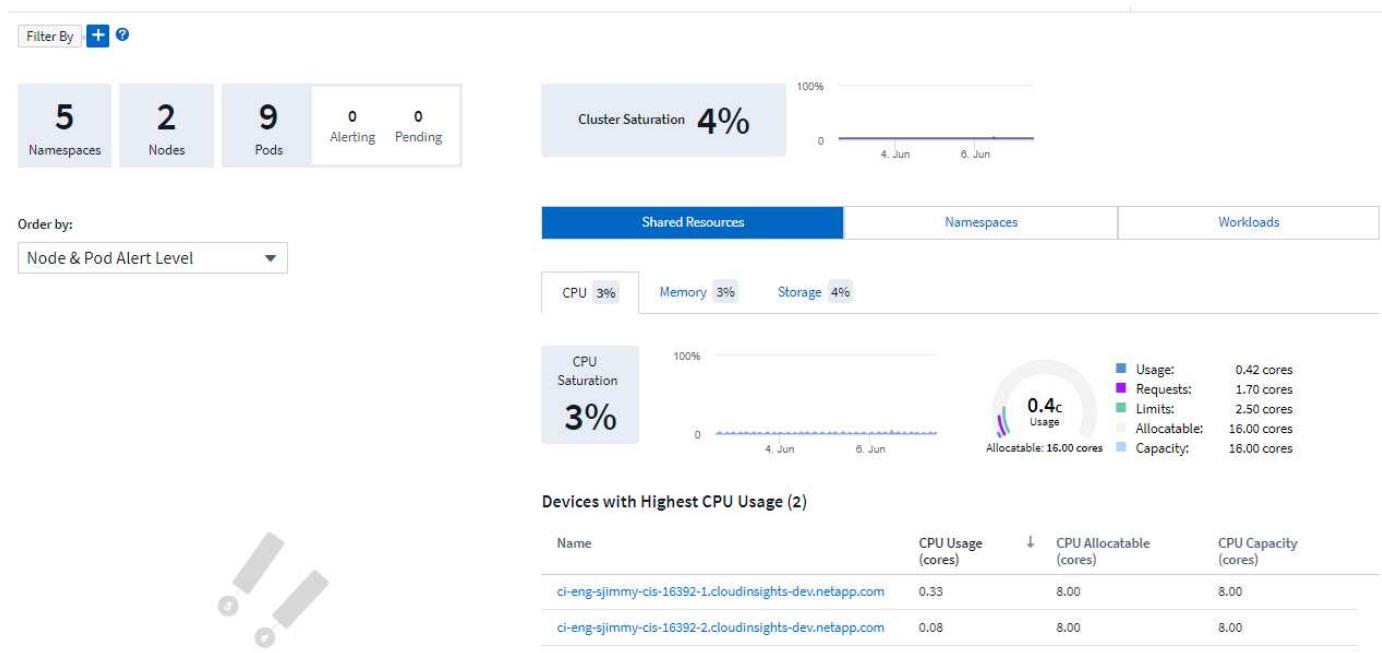
Filters based on wildcards or expressions (e.g. NOT, AND, "None", etc.) display in dark blue in the filter field. Items that you select directly from the list are displayed in light blue.

Kubernetes filters are contextual, meaning for example that if you are on a specific node page, the pod_name filter only lists pods related to that node. Moreover, if you apply a filter for a specific namespace, then the pod_name filter will list only pods on that node *and* in that namespace.

Note that Wildcard and Expression filtering works with text or lists but not with numerics, dates or booleans.

Kubernetes Cluster Detail Page

The Kubernetes cluster detail page displays a detailed overview of your Kubernetes cluster.



Namespace, Node, and Pod Counts

The counts at the top of the page show you the total number of namespaces, nodes, and pods in the cluster, as well as the number of pods that are currently alerting and pending.

Shared Resources and Saturation

On the top right of the detail page is your cluster saturation as a current percentage as well as a graph showing the recent trend over time. Cluster saturation is the highest of CPU, memory, or storage saturation at each point in time.

Below that, the page shows by default **Shared Resources** usage, with tabs for CPU, Memory, and Storage. Each tab shows the saturation percentage and trend over time, with additional usage details. For storage, the value shown is the greater of backend and filesystem saturation, which are calculated independently.

The devices with the highest usage are shown in a table at the bottom. Click any link to explore these devices.

Namespaces

The Namespaces tab displays a list of all the namespaces in your Kubernetes environment, showing CPU and Memory usage as well as a count of workloads in each namespace. Click the Name links to explore each namespace.

Shared Resources	Namespaces	Workloads
------------------	------------	-----------

Namespaces (5)

Name ↓	CPU Usage (cores)	Memory Usage (GiB)	Workload Count
netapp-monitoring	0.25	0.38	4
kube-system	0.01	0.03	3
kube-public	0.00	0.00	0
kube-node-lease	0.00	0.00	0
default	0.00	<0.01	1

Workloads

Similarly, the Workloads tab displays a list of the workloads in each namespace, again showing CPU and Memory usage. Clicking the Namespace links drills into each.

Shared Resources	Namespaces	Workloads
------------------	------------	-----------

Workloads (8)

Name ↓	CPU Usage (cores)	Memory Usage (GiB)	Namespace
telegraf-rs-lf9gg	0.24	0.24	netapp-monitoring
telegraf-ds-k957c	0.01	0.10	netapp-monitoring
nginx	0.00	<0.01	default
monitoring-operator-6fcf4755ff-p2cs6	<0.01	0.02	netapp-monitoring
metrics-server-7b4f8b595-f7j9f	<0.01	0.01	kube-system
local-path-provisioner-64d457c485-289gx	<0.01	0.01	kube-system
kube-state-metrics-7995866f8c-t8c49	<0.01	0.01	netapp-monitoring
coredns-5d69dc75db-nkw5p	<0.01	0.01	kube-system

The Cluster "Wheel"



The Cluster "Wheel" section provides node and pod health at a glance, which you can drill into for more information. If your cluster contains more nodes than can be displayed in this area of the page, you will be able to turn the wheel using the buttons available.

Alerting pods or nodes are displayed in red. "Warning" areas are displayed in orange. Pods that are unscheduled (that is, unattached) will display in the lower corner of the Cluster "Wheel".

Hovering over a pod (circle) or Node (bar) will extend the view of the node.



Clicking on the pod or node in that view will zoom in to the expanded Node view.



From here, you can hover over an element to display details about that element. For example, hovering over the critical pod in this example displays details about that pod.



You can view Filesystem, Memory, and CPU information by hovering over the Node elements.



A note about the gauges

The Memory and CPU gauges show three colors, since they show *used* in relation to both *allocatable capacity* and *total capacity*.

ONTAP Essentials

ONTAP Essentials is a set of dashboards and workflows that provide detailed overviews of your ONTAP inventories and workloads. You may see the following terms used when working in ONTAP Essentials:

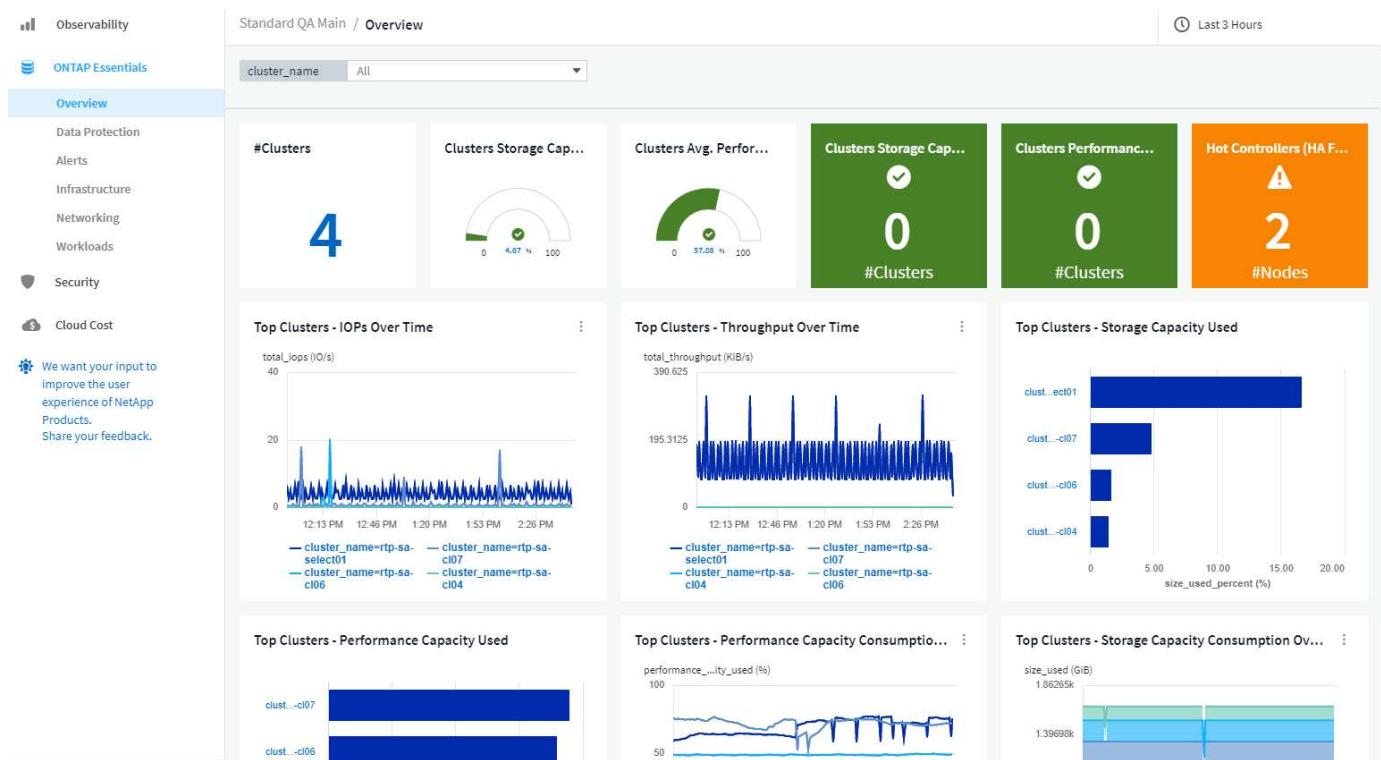
- Infrastructure/Inventory: Objects that provide storage/networking services to user data
- Workloads: Objects that provide interface to users to read/write data.
- Data Protection: Objects that can be protected using NetApp data protection technologies

For additional terms and definitions related to ONTAP, see the [ONTAP Data Collector](#) documentation.

ONTAP Essentials requires at least one working ONTAP data collector with data collected within the last seven days.

Overview

To begin exploring, select **ONTAP Essentials** from the main Cloud Insights menu.



The **Overview** dashboard displays useful information like the number of clusters in your environment with their overall capacity and performance percentages. You will also see predictive data regarding the number of expected days until storage capacity or performance capacity runs out of space. Additionally, if any controllers in your infrastructure are running with their CPU at more than 65%--potentially putting your cluster at risk in case of failover—ONTAP Essentials shows those as "Hot" controllers.

Informative graphs give you a look into performance over time as well as breakdowns of capacity usage.

Each of these graphs or data points can be used as a starting point for exploration or investigation.

Note: A "days to full" number of "0" (zero) indicates that days to full is estimated at greater than 90 days. In other words, your systems aren't in danger of running out of space any time soon.

Data Protection

Select the **Data Protection** page to view SnapMirror relationships. Click through to source or destination volume information, or click the gear icon to add columns for the data you wish to view.

hhndks4 / Data-protection / All Relationships - Protection Last 3 Hours

netapp_ontap.snapmirror ▾ All Relationships ▾

Filter By cluster_vendor NetApp x x + ?

Group netapp_ontap.snapmirror x x

28 items found

Table Row Grouping	Metrics & Attributes
netapp_ontap.snapmirror	relationship... ↑ is_healthy lag_time (sec) last_successful_u... policy_name source.volume_n... destination.vol...
dpsvm01:leafy_SL_unified_dest_01	idle ✓ N/A MirrorAndVault leafy_SL_unified_...
dpsvm01:dpsvm01_vol_NSLSM_VOL_LUN_1592:	idle ✓ 1,842.00 2022-07-27 13:35:0... XDPDefault vol_NSLSM_VOL_L... dpsvm01_vol_NSLS...
dpsvm01:a_demo_volume_dest01	idle ✓ 142.00 2022-07-27 13:35:0... LEAFYSLVAULT a_demo_volume_...
mattsrv07:mattsrv07_volume3	idle ✓ 2022-07-13 20:08:1... SVM-DR-identity-p... mattsrv07_volum...
dpsvm01:rtp_demo_01_leafydemo01_Asynchr	idle ✓ 11,107,543.00 2022-07-27 13:10:0... XDPDefault rtp_demo_01_lea...
rtp-sa-cl07-svm-01:test_Phil_mirror_create_tes	idle ✓ 135,033,424.00 N/A MirrorAllSnapshots test_Phil_mirror_c...
mattsrv07:mattsrv07_volume4	idle ✓ 2022-07-13 20:08:1... SVM-DR-identity-p... mattsrv07_volum...
dpsvm01:vol_LEAFTYDEMOLUN01_dest	idle ✓ 1,843.00 2022-07-27 13:05:0... Asynchronous vol_LEAFTYDEMOL...
rtp-sa-cl07-svm-01:mirror_samplesource1_dest	idle ✓ 1,843.00 2022-07-27 13:05:0... Asynchronous mirror_samplesou...
astra_301:vol1_dp	idle ✓ 8,299,460.00 N/A XDPDefault vol1 vol1_dp
rtp-sa-cl07-svm-01:vol_pgb_sm_fanout_srcsv_	idle ✓ 48,343.00 2022-07-27 00:10:0... pgb_mirror_vault vol_pgb_sm_fano...

Alerts

Here you can view the Active alerts in your environment and quickly drill down into potential problems. Select the *Resolved* tab to view alerts that have been resolved.

 **ONTAP Essentials**

[Overview](#)

[Data Protection](#)

Alerts

[Infrastructure](#)

[Networking](#)

[Workloads](#)

[Active \(86\)](#) [Resolved \(0\)](#)

Alerts (86)							
alertId	triggeredTime ↓	currentSeverity	monitor	triggeredOn	status	hasCorrective Actions	Change All Alerts Status
AL-356704	12 hours ago Sep 9, 2022 2:16 AM	critical	Snapshot Reserve Space ...	cluster_name:rtp-sa-cl04 vserver_name:test_ran volume_name:thick_vol_2 cluster_uuid:f34cd2c8-f1b3-11e9-b97f-00a0985f6587 cluster_vendor:NetApp cluster_model:AFF8040	New	✓	
AL-355988	a day ago Sep 8, 2022 11:00 AM	warning	User Quota Capacity Soft ...	cluster_name:rtp-sa-cl06 volume:qtreevol1 quota_type:user user_or_group:16716 cluster_uuid:da294f0d-ad92-11e6-9969-00a0987b8fe8 cluster_vendor:NetApp cluster_model:FAS2552	New	✓	

Infrastructure

The ONTAP Essentials **Infrastructure** page gives you a view of cluster health and performance, using pre-built (yet further customizable) queries on all the basic ONTAP objects. Select the object type you wish to explore (cluster, storage pool, etc.) and choose whether to view health or performance information. Set filters to dive deeper into individual systems.

-service-multi... / Infrastructure / **All Storage Pools - Health**

netapp_ontap.aggregate ▾ **All Storage Pools**

Filter By: cluster_vendor Group: netapp_ontap.aggregate

Health

- All Storage Pools**
- Performance
- All Storage Pools
- Capacity
- All Storage Pools

1 items found

Table Row Grouping	Metrics & Attributes
netapp_ontap.aggregate	ndd

harvest_astra_aggr1

aggr_SnapLock_02

hdd

Infrastructure page showing cluster health:

hhndks4 / Infrastructure / **All Clusters - Health**

Observability

ONTAP Essentials

- Overview
- Data Protection
- Infrastructure**
- Workloads

Security

We want your input to improve the user experience of NetApp Products. Share your feedback.

netapp_ontap.cluster ▾ **All Clusters**

Filter By: cluster_vendor NetApp Group: netapp_ontap.cluster

3 items found

Table Row Grouping	Metrics & Attributes	cluster_version	node_count	cluster_location
netapp_ontap.cluster	fips_enabled ↑	NetApp Release 9.8P13: Fri Jul 15 22:00:00 UTC 2022	2	SA East Lab, RTP 1.3, Jxx
rtp-sa-cl07	false	NetApp Release 9.9.1P9X3: Tue Apr 1 10:00:00 UTC 2023	2	GDL QQ 22
umeng-aff300-05-06	false	NetApp Release Metropolitan_9.11.1: Mon Mar 13 10:00:00 UTC 2023	2	GDL
umeng-aff300-01-02	false	NetApp Release Metropolitan_9.11.1: Mon Mar 13 10:00:00 UTC 2023	2	GDL

Networking

ONTAP Essentials Networking gives you views into your FC, NVME FC, Ethernet, and iSCSI infrastructure. On these pages you can explore things like ports in your clusters and their nodes.

The screenshot shows the ONTAP Essentials interface with the 'Alerts' tab selected. At the top, there are tabs for 'Overview', 'Data Protection', 'Alerts', 'Infrastructure', 'Networking', and 'Workloads'. Below the tabs is a search bar with filters: triggeredOn (NetApp), status (New, In process), currentSeverity (Warning, Critical), and a button to '+ Add'. Below the search bar is a table titled 'Alerts (86)'. The table has columns: alertId, triggeredTime, currentSeverity, monitor, triggeredOn, status, and hasCorrectiveActions. Two rows are visible:

alertId	triggeredTime	currentSeverity	monitor	triggeredOn	status	hasCorrectiveActions
AL-356704	12 hours ago Sep 9, 2022 2:16 AM	⚠ Critical	Snapshot Reserve Space ...	cluster_name: rtp-sa-cl04 vserver_name: test_ran volume_name: thick_vol_2 cluster_uuid: f34cd2c8-f1b3-11e9-b97f-00a0985f6587 cluster_vendor: NetApp cluster_model: AFF8040	New	✓
AL-355988	a day ago Sep 8, 2022 11:00 AM	⚠ Warning	User Quota Capacity Soft ...	cluster_name: rtp-sa-cl06 volume: qtrevol1 quota_type: user user_or_group: 16716 cluster_uuid: da294f0d-ad92-11e6-9969-00a0987b8fe8 cluster_vendor: NetApp cluster_model: FAS2552	New	✓

Workloads

View and explore workloads on LUNs/Volumes, NFS or SMB Shares, or Qtrees in your environment.

The screenshot shows the ONTAP Essentials interface with the 'Workloads' tab selected. At the top, there are tabs for 'Overview', 'Data Protection', 'Infrastructure', 'Workloads', and 'Security'. A lock icon is also present. A dropdown menu for 'Workloads' is open, showing 'LUNs / Volumes' and 'Qtrees'.

netapp_ontap.lun ▼ All LUNs

Filter By cluster_vendor NetApp X X + ?

Group netapp_ontap.lun X X

13 items found

Table Row Grouping Metrics & Attributes

netapp_ontap.lun	total_late... ↑	total_iops (IOP/s)	total_throughput (MB/s)	size (B)	size_used (B)	volume	vserver_name	aggregate_name	node
/vol/ste/ste	0.00	0.00	0.00	53,694,627,840... 0.00	0.00	ste	vs_test	umeng_aff300...	ui
/vol/kubebug/kubebuglun1	0.00	0.00	0.00	85,905,637,376... 1,489,985,536.00	1,489,985,536.00	kubebug	vs_test	umeng_aff300...	ui
/vol/trident_pvc_3ef5a87c_4149_44e8_8113...	0.00	0.00	0.00	1,073,741,824.00	0.00	trident_pvc_3e...	vs_test	umeng_aff300...	ui
/vol/trident_pvc_0bf4ffd4_3f11_4d63_aa01_...	0.00	0.00	0.00	1,073,741,824.00	0.00	trident_pvc_0b...	vs_test	umeng_aff300...	ui
/vol/NSLM_VOL_LUN_1597772263794/matts...	0.00	0.00	0.00	1,073,741,824.00	0.00	NSLM_VOL_LU...	VMware_test	aggr_data_01...	rt
/vol/mattlun12345/mattlun12345	0.00	0.00	0.00	1,073,741,824.00	0.00	mattlun12345	VMware_test	aggr_data_01...	rt
/vol/kubebug1/kubebuglun2	0.00	0.00	0.00	85,904,826,368... 0.00	0.00	kubebug1	vs_test	umeng_aff300...	ui
/vol/trident_pvc_d66d7f51_a623_4fc3_8cd...	0.00	0.00	0.00	1,073,741,824.00	0.00	trident_pvc_d6...	vs_test	umeng_aff300...	ui
/vol/Rah/Rah	0.00	0.00	0.00	57,576,960.00	0.00	Rah	vs_test	umeng_aff300...	ui
/vol/chap_test_lun/vol/chap_test_lun	0.00	0.00	0.00	107,374,182,40... 0.00	0.00	chap_test_lun_...	VMware_test	aggr_data_01...	rt
/vol/windows_iscsi_example/windows_iscsi...	0.00	0.00	1.04	1,073,741,824.00	10,911,744.00	windows_iscsi...	VMware_test	aggr_data_01...	rt
/vol/vol_test/lun1	0.04	0.10	0.00	1,073,741,824.00	0.00	vol_test	vs_test	umeng_aff300...	ui
/vol/osc_iscsi_vol01/osc_iscsi_vol01	2.11	116.83	2,737,374.33	4,398,046,511,1... 2,535,381,008,3...	2,535,381,008,3...	osc_iscsi_vol01	osc	umeng_aff300...	ui

Working with Queries

Assets used in queries

Queries enable you to monitor and troubleshoot your network by searching the assets and metrics in your environment at a granular level based on user-selected criteria (for example, annotations).

Note that annotation rules, which automatically assign annotations to assets, *require* a query.

You can query the physical or virtual inventory assets (and their associated metrics) in your environment, or the metrics provided with integration such as Kubernetes or ONTAP Advanced Data.

Inventory Assets

The following asset types can be used in queries, dashboard widgets, and custom asset landing pages. The fields and counters available for filters, expressions, and display will vary among asset types. Not all assets can be used in all widget types.

- Application
- Datastore
- Disk
- Fabric
- Generic Device
- Host
- Internal Volume
- iSCSI Session
- iSCSI Network Portal
- Path
- Port
- Qtree
- Quota
- Share
- Storage
- Storage Node
- Storage Pool
- Storage Virtual Machine (SVM)
- Switch
- Tape
- VMDK
- Virtual Machine
- Volume

- Zone
- Zone Member

Integration Metrics

In addition to querying for inventory assets and their associated performance metrics, you can query for **integration data** metrics as well, such as those generated by Kubernetes or Docker, or provided with ONTAP Advanced Metrics.



Creating Queries

Queries enable you to search the assets in your environment at a granular level, allowing to filter for the data you want and sort the results to your liking.

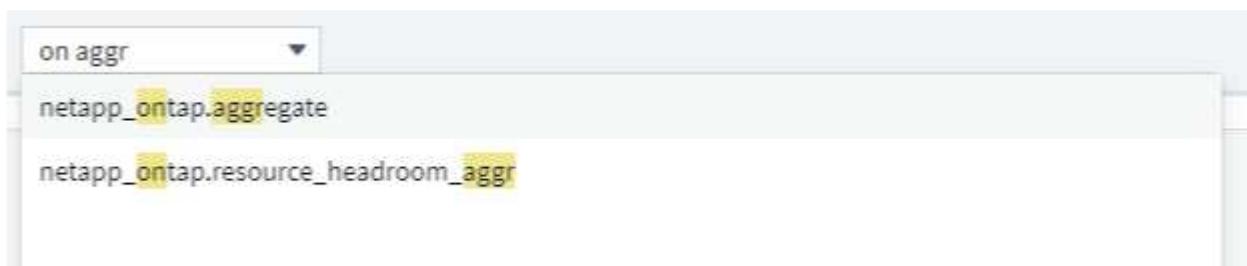
For example, you can create a query for *volumes*, add a filter to find particular *storages* associated with the selected volumes, add another filter to find a particular *annotation* such as "Tier 1" on the selected storages, and finally add another filter to find all storages with *IOPS - Read (IO/s)* greater than 25. When the results are displayed, you can then sort the columns of information associated with the query in ascending or descending order.

Note: When a new data collector is added which acquires assets, or any annotation or application assignments are made, you can query for those new assets, annotations, or applications only after the queries are indexed. Indexing occurs at a regularly scheduled interval or during certain events such as running annotation rules.

Creating a Query is very simple:

1. Navigate to **Queries > *+New Query**.
2. From the 'Select...' list, select the object type you want to query for. You can scroll through the list or you can start typing to more quickly find what you're searching for.

Scroll list:

**Type-to-Search:**

You can add filters to further narrow down your query by clicking the **+** button in the **Filter By** field. Group rows by object or attribute. When working with integration data (Kubernetes, ONTAP Advanced Metrics, etc.), you can group by multiple attributes, if desired.

netapp_ontap.aggregate

Filter By cluster_name ci- +

Group aggr_name x

5 items found

Table Row Grouping		Metrics & Attributes	
aggr_name		cp_read_blocks	cluster_name ↓
oci02sat0		0.59	oci-phonehome
oci02sat1		0.15	oci-phonehome
oci02sat2		212.64	oci-phonehome
oci01sat0		0.39	oci-phonehome
oci01sat1		48.89	oci-phonehome

The query results list shows a number of default columns, depending on the object type searched for. To add, remove, or change the columns, click the gear icon on the right of the table. The available columns vary based on the asset/metric type.

netapp_ontap.aggregate

Filter By +

Group aggr_name x

14 items found

Table Row Grouping		Metrics & Attributes	
aggr_name		cp_read_blocks	agent_version ↑
aggr0_optimus_02		1.72	Apache-HttpClient
aggr1_optimus_02		408.84	Apache-HttpClient
ocinaneqa1_04_aggr0		6.19	Apache-HttpClient
ocinaneqa1_03_aggr0		6.48	Apache-HttpClient
oci02sat0		1.04	Apache-HttpClient

- Show Selected Only
- agent_version
- aggr_name
- cluster_location
- cluster_name
- cluster_serial_number
- cluster_version

After you have configured your query to show you the results you want, you can click the **Save** button to save the query for future use. Give it a meaningful and unique name.

More on Filtering

Wildcards and Expressions

When you are filtering for text or list values in queries or dashboard widgets, as you begin typing you are presented with the option to create a **wildcard filter** based on the current text. Selecting this option will return all results that match the wildcard expression. You can also create **expressions** using NOT or OR, or you can select the "None" option to filter for null values in the field.

kubernetes.pod X ▾

Filter By pod_name ingest X + ?

Group pod_name X Create wildcard containing "ingest"

71 items found

Table Row Grouping

ci-service-datalake-ingestion-85b5bdfd6d-2qbwr
service-foundation-ingest-767dfd5bfc-vxd5p
None

Filters based on wildcards or expressions (e.g. NOT, OR, "None", etc.) display in dark blue in the filter field. Items that you select directly from the list are displayed in light blue.

kubernetes.pod X ▾

Filter By pod_name *ingest* X ci-service-audit-5f775dd975-brfdc X X ▾ + ?

Group pod_name X X ▾

3 items found

Table Row Grouping

pod_name

ci-service-audit-5f775dd975-brfdc

ci-service-datalake-ingestion-85b5bdfd6d-2qbwr

service-foundation-ingest-767dfd5bfc-vxd5p

Note that Wildcard and Expression filtering works with text or lists but not with numerics, dates or booleans.

Refining Filters

You can use the following to refine your filter:

Filter	What it does	Example	Result
--------	--------------	---------	--------

* (Asterisk)	enables you to search for everything	vol*rhel	returns all resources that start with "vol" and end with "rhel"
? (question mark)	enables you to search for a specific number of characters	BOS-PRD??-S12	returns BOS-PRD12-S12, BOS-PRD23-S12, and so on
OR	enables you to specify multiple entities	FAS2240 OR CX600 OR FAS3270	returns any of FAS2440, CX600, or FAS3270
NOT	allows you to exclude text from the search results	NOT EMC*	returns everything that does not start with "EMC"
<i>None</i>	searches for NULL values in all fields	<i>None</i>	returns results where the target field is empty
Not *	searches for NULL values in <i>text-only</i> fields	Not *	returns results where the target field is empty

If you enclose a filter string in double quotes, Insight treats everything between the first and last quote as an exact match. Any special characters or operators inside the quotes will be treated as literals. For example, filtering for "*" will return results that are a literal asterisk; the asterisk will not be treated as a wildcard in this case. The operators OR and NOT will also be treated as literal strings when enclosed in double quotes.

What do I do now that I have query results?

Querying provides a simple place to add annotations or assign applications to assets. Note that you can only assign applications or annotations to your inventory assets (Disk, Storage, etc.). Integration metrics cannot take on annotation or application assignments.

To assign an annotation or application to the assets resulting from your query, simply select the asset(s) using the check box column on the left of the results table, then click the **Bulk Actions** button on the right. Choose the desired action to apply to the selected assets.

The screenshot shows the Insight interface with a query results table. At the top, there's a search bar labeled 'Volume' and a filter bar with 'Filter By' set to 'Name' and 'Any'. Below the table, a context menu is open over two selected assets, showing options like 'Add Annotation', 'Remove Annotation', 'Add Application', and 'Remove Application'. The table has columns for Name, Storage Pools, Capacity - Raw (GB), and Mapped Ports. The selected assets are DmoSAN_optimus:hoffma... and DmoSAN_optimus:mc_D... Both have 'Add Annotation' selected.

Name ↑	Storage Pools	Capacity - Raw (GB)	Mapped Ports
DmoESX_optimus:mc_Dm...	optimus-02:aggr1_optimu...	N/A	
<input checked="" type="checkbox"/> DmoSAN_optimus:hoffma...	optimus-02:aggr1_optimu...	N/A	
<input checked="" type="checkbox"/> DmoSAN_optimus:mc_D...	optimus-02:aggr1_optimu...	N/A	
oci-3070-01:/vol/vfiler_lun...	oci-3070-01:aggr5	N/A	OS:windows
spectrav1:sjimmylscsi:/v...	ocinaneqa1-01:spectraaggr1	N/A	OS:linux

Annotation Rules require query

If you are configuring [Annotation Rules](#), each rule must have an underlying query to work with. But as you've seen above, queries can be made as broad or as narrow as you need.

Viewing queries

You can view your queries to monitor your assets and change how your queries display the data related to your assets.

Steps

1. Log in to your Cloud Insights tenant.
2. Click **Queries** and select **Show all queries**.

You can change how queries display by doing any of the following:

3. You can enter text in the filter box to search to display specific queries.
4. You can change the sort order of the columns in the table of queries to either ascending (up arrow) or descending (down arrow) by clicking the arrow in the column header.
5. To resize a column, hover the mouse over the column header until a blue bar appears. Place the mouse over the bar and drag it right or left.
6. To move a column, click on the column header and drag it right or left.

When scrolling through the query results, be aware that the results may change as Cloud Insights automatically polls your data collectors. This may result in some items being missing, or some items appearing out of order depending on how they are sorted.

Exporting query results to a .CSV file

You can export the results of any query to a .CSV file, which will allow you to analyze the data or import it into another application.

Steps

1. Log in to Cloud Insights.
2. Click **Queries** and select **Show all queries**.

The Queries page is displayed.

3. Click a query.
4. Click  to export the query results to a .CSV file.



Export to .CSV is also available in the "three dots" menu in dashboard table widgets as well as most landing page tables.

The exported data will reflect the current filtering, columns, and column names displayed.

Note: When a comma appears in an asset name, the export encloses the name in quotes, preserving the asset name and the proper .csv format.

When opening an exported .CSV file with Excel, if you have an object name or other field that is in the format NN:NN (two digits followed by a colon followed by two more digits), Excel will sometimes interpret that name as a Time format, instead of Text format. This can result in Excel displaying incorrect values in those columns. For example, an object named "81:45" would show in Excel as "81:45:00".

To work around this, import the .CSV into Excel using the following steps:

1. Open a new sheet in Excel.
2. On the "Data" tab, choose "From Text".
3. Locate the desired .CSV file and click "Import".
4. In the Import wizard, choose "Delimited" and click Next.
5. Choose "Comma" for the delimiter and click Next.
6. Select the desired columns and choose "Text" for the column data format.
7. Click Finish.

Your objects should show in Excel in the proper format.

Modifying or Deleting a Query

Modifying a Query

You can change the criteria that are associated with a query when you want to change the search criteria for the assets that you are querying.

Steps

1. Click **Queries** and select **Show all queries**.

The Queries page is displayed.

2. Click the query name
3.
To add a criteria to the query, click  and select a criteria from the list.
4. To remove a filter from the query, click the **X** next to the filter to remove.

When you have made all necessary changes, do one of the following:

- Click the **Save** button to save the query with the name that was used initially.
- Click the drop-down next to the **Save** button and select **Save As** to save the query with another name. This does not overwrite the original query.
- Click the drop-down next to the **Save** button and select **Rename** to change the query name that you had used initially. This overwrites the original query.
- Click the drop-down next to the **Save** button and select **Discard Changes** to revert the query back to the last saved changes.

Deleting a Query

To delete a query, click **Queries** and select **Show all queries**, and do one of the following:

1. Click on the "three dot" menu to the right of the query and click **Delete**.
2. Click on the query name and select **Delete** from the **Save** drop-down menu.

Assigning multiple applications to or removing multiple applications from assets

You can assign multiple [applications](#) to or remove multiple applications from assets by using a query instead of having to manually assign or remove them.



You can use these steps to add or remove [annotations](#) in the same way.

Before you begin

You must have already created a query that finds all the assets that you want to edit.

Steps

1. Click **Queries** and select **Show all queries**.

The Queries page displays.

2. Click the name of the query that finds the assets.

The list of assets associated with the query displays.

3. Select the desired assets in the list or click the top checkbox to select All.

The **Bulk Actions ▾** button displays.

- 4.

To add an application to the selected assets, click **Bulk Actions ▾** and select **Add Application**.

5. Select one or more applications.

You can select multiple applications for hosts, internal volumes, qtrees, and virtual machines; however, you can select only one application for a volume or a share.

6. Click **Save**.

- 7.

To remove an application assigned to the assets, click **Bulk Actions ▾** and select **Remove Application**.

8. Select the application or applications you want to remove.

9. Click **Delete**.

Any new applications you assign override any applications on the asset that were derived from another asset. For example, volumes inherit applications from hosts, and when new applications are assigned to a volume, the new application takes precedence over the derived application.

After you click **Save** on a bulk add or **Remove** on a bulk delete action, Cloud Insights informs you that the action will take some time. You can dismiss this message; the action will continue in the background.



For environments with large amounts of related assets, inheritance of application assignments to those assets could take several minutes. Please allow more time for inheritance to occur if you have many related assets.

Copying table values

You can copy values in tables to the clipboard for use in search boxes or other applications.

About this task

There are two methods you can use to copy values from tables or query results to the clipboard.

Steps

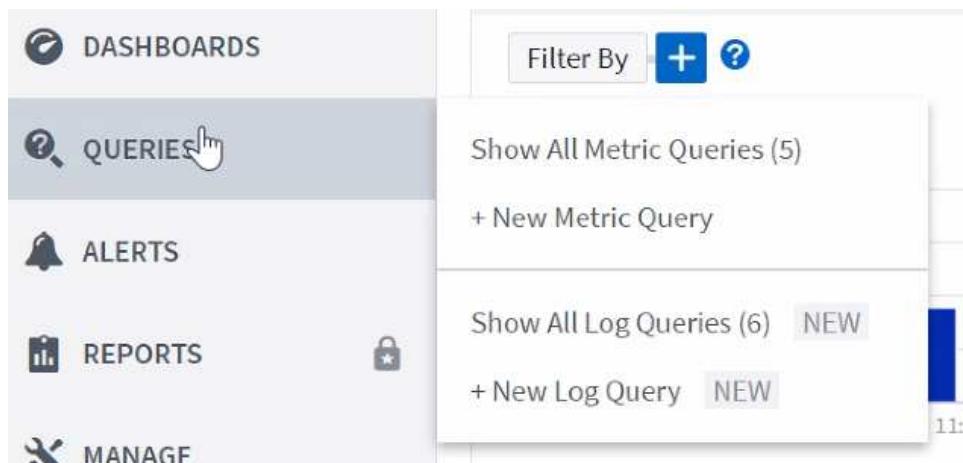
1. Method 1: Highlight the desired text with the mouse, copy it, and paste it into search fields or other applications.
2. Method 2: For single-value fields, hover over the field and click the clipboard icon  that appears. The value is copied to the clipboard for use in search fields or other applications.

Note that only values that are links to assets can be copied using this method. Only fields that include single values (i.e. non-lists) have the copy icon.

Log Explorer

The Cloud Insights Log Explorer is a powerful tool for querying system logs. In addition to helping with investigations, you can also save a log query in a Monitor to provide alerts when those particular log triggers are activated.

To begin exploring logs, click **Queries > +New Log Query**.



Select an available log from the list.

Select...

- logs.kubernetes
- logs.kubernetes.events
- logs.netapp.ems
- logs.ontapems
- logs.syslog



The types of logs available for querying may vary based on your environment. Additional log types may be added over time.

You can set filters to further refine the results of the query. For example, to find all log messages showing a failure, set a filter for *Messages* containing the word "failed".



You can begin typing the desired text in the filter field; Cloud Insights will prompt you to create a wildcard search containing the string as you type.

The results are displayed in a graph showing the number of log instances in each time period shown. Below the graph are the log entries themselves. The graph and the entries refresh automatically based on the selected time range.



The Log Graph

The graph shows the number of log entries, grouped into *buckets*, which are based on the selected dashboard time range. The buckets for each time range are as follows:

Dashboard Time Range	Bucket size
Last 15 Minutes	10 Seconds
Last 30 Minutes	15 Seconds
Last 60 Minutes	30 Seconds
Last 2 Hours	1 Minute
Last 3 Hours	5 Minutes
Last 6 Hours	5 Minutes
Last 12 Hours	10 Minutes
Last 24 Hours	15 Minutes
Last 2 Days	30 Minutes
Last 3 Days	45 Minutes
Last 7 Days	2 Hours
Last 30 Days	1 Day

To zoom in the graph, simply drag the sliders from either side. To pan the zoomed area, click and hold in the white area and move left or right. Click *Reset Zoom* to reset the zoom level.



Note that when zooming the graph or scrolling the table, dashboard auto-refresh will pause and the time range will show the frozen time. To resume refresh, click the *Resume* button . This will also reset the zoom level.

At any point, you can click on *Create a Log Monitor* to create a new Monitor based on the current filter.

Log Details

Clicking anywhere in a log entry in the list will open a detail pane for that entry. Here you can explore more information about the event.

Click on "Add Filter" to add the selected field to the current filter. The log entry list will update based on the new filter.

Log Details



timestamp

09/20/2021 9:03:36 PM

message

2021-09-20T15:33:36Z E! [processors.execd] stderr: "Total time to process mountstats file: /hostfs/proc/1/mountstats, was: 0s"

id: 227814532095936770

node_name: ci-auto-dsacq-insights-1.cloudinsights-dev.netapp.com

Add Filter



source: telegraf-ds-dfcc5

type: logs.kubernetes

kubernetes

kubernetes.annotations.openshift.io_scc:

kubernetes.container_hash: ci-registry.name.openenglab.netapp.com:8022/telegraf@sha256:00h45a7cc0761c

Troubleshooting

Here you will find suggestions for troubleshooting problems with Log Queries.

Problem:	Try this:
I don't see "debug" messages in my log query	Debug log messaging is not collected. To capture messages you want, change the relevant message severity to <i>informational</i> , <i>error</i> , <i>alert</i> , <i>emergency</i> , or <i>notice</i> level.

Working with Annotations

Defining annotations

When customizing Cloud Insights to track data for your corporate requirements, you can define specialized notes, called annotations, and assign them to your assets.

You can assign annotations to assets with information such as asset end of life, data center, building location, storage tier, or volume service level.

Using annotations to help monitor your environment includes the following high-level tasks:

- Creating or editing definitions for all annotation types.
- Displaying asset pages and associating each asset with one or more annotations.

For example, if an asset is being leased and the lease expires within two months, you might want to apply an end-of-life annotation to the asset. This helps prevent others from using that asset for an extended time.

- Creating rules to automatically apply annotations to multiple assets of the same type.
- Filter assets by their annotations.

Default annotation types

Cloud Insights provides some default annotation types. These annotations can be used to filter or group data.

You can associate assets with default annotation types such as the following:

- Asset life cycle, such as birthday, sunset, or end of life
- Location information about a device, such as data center, building, or floor
- Classification of assets, such as by quality (tiers), by connected devices (switch level), or by service level
- Status, such as hot (high utilization)

The following table lists the Cloud Insights-provided annotation types.

Annotation types	Description	Type
Alias	User-friendly name for a resource	Text
Compute Resource Group	Group assignment used by the Host and VM Filesystems data collector	List
Data Center	Physical location	List
Hot	Devices under heavy use on a regular basis or at the threshold of capacity	Boolean
Note	Comments associated with a resource	Text
Service Level	A set of supported service levels that you can assign to resources. Provides an ordered options list for internal volumes, qtree, and volumes. Edit service levels to set performance policies for different levels.	List

Sunset	Threshold set after which no new allocations can be made to that device. Useful for planned migrations and other pending network changes.	Date
Switch Level	Predefined options for setting up categories for switches. Typically, these designations remain for the life of the device, although you can edit them. Available only for switches.	List
Tier	Can be used to define different levels of service within your environment. Tiers can define the type of level, such as speed needed (for example, gold or silver). This feature is available only on internal volumes, qtrees, storage arrays, storage pools, and volumes.	List
Violation Severity	Rank (for example, major) of a violation (for example, missing host ports or missing redundancy), in a hierarchy of highest to lowest importance.	List



Alias, Data Center, Hot, Service Level, Sunset, Switch Level, Tier, and Violation Severity are system-level annotations, which you cannot delete or rename; you can change only their assigned values.

Creating custom annotations

Using annotations, you can add custom business-specific data that matches your business needs to assets. While Cloud Insights provides a set of default annotations, you might find that you want to view data in other ways. The data in custom annotations supplements device data already collected, such as storage manufacturer, number volumes, and performance statistics. The data you add using annotations is not discovered by Cloud Insights.

Steps

1. In the Cloud Insights menu, click **Manage > Annotations**.

The Annotations page displays the list of annotations.

2. Click **+Add**
3. Enter a **Name** and **Description** of the annotation.

You can enter up to 255 characters in these fields.

4. Click **Type** and then select one of the following options that represents the type of data allowed in this annotation:

Annotation types

Boolean

Creates a drop-down list with the choices of yes and no. For example, the "Direct Attached" annotation is Boolean.

Date

This creates a field that holds a date. For example, if the annotation will be a date, select this.

List

Creates either of the following:

- A drop-down fixed list

When others are assigning this annotation type on a device, they cannot add more values to the list.

- A drop-down flexible list

If you select the Add new values on the fly option when you create this list, when others are assigning this annotation type on a device, they can add more values to the list.

Number

Creates a field where the user assigning the annotation can enter a number. For example, if the annotation type is "Floor", the user could select the Value Type of "number" and enter the floor number.

Text

Creates a field that allows free-form text. For example, you might enter "Language" as the annotation type, select "Text" as the value type, and enter a language as a value.



After you set the type and save your changes, you cannot change the type of the annotation. If you need to change the type, you have to delete the annotation and create a new one.

1. If you select List as the annotation type, do the following:

- a. Select **Add new values on the fly** if you want the ability to add more values to the annotation when on an asset page, which creates a flexible list.

For example, suppose you are on an asset page and the asset has the City annotation with the values Detroit, Tampa, and Boston. If you selected the **Add new values on the fly** option, you can add additional values to City like San Francisco and Chicago directly on the asset page instead of having to go to the Annotations page to add them. If you do not choose this option, you cannot add new annotation values when applying the annotation; this creates a fixed list.

- b. Enter a value and description in **Value** and **Description** fields.
- c. Click **Add** to add additional values.
- d. Click the Trash icon to delete a value.

2. Click **Save**

Your annotations appear in the list on the Annotations page.

After you finish

In the UI, the annotation is available immediately for use.

Using annotations

You create annotations and assign them to assets you monitor. Annotations are notes that provide information about an asset, such as physical location, end of life, storage tier, or volume service levels.

Defining annotations

Using annotations, you can add custom business-specific data that matches your business needs to assets. While Cloud Insights provides a set of default annotations, such as asset life cycle (birthday or end of life), building or data center location, and tier, you might find that you want to view data in other ways.

The data in custom annotations supplements device data already collected, such as switch manufacturer, number of ports, and performance statistics. The data you add using annotations is not discovered by Cloud Insights.

Before you begin

- List any industry terminology to which environment data must be associated.
- List corporate terminology to which environment data must be associated.
- Identify any default annotation types that you might be able to use.
- Identify which custom annotations you need to create. You need to create the annotation before it can be assigned to an asset.

Use the following steps to create an annotation.

Steps

1. In the Cloud Insights menu, click **Manage > Annotations**
2. Click **+ Annotation** to create a new annotation.
3. Enter a Name, Description, and type for the new annotation.

For example, enter the following to create a text annotation that defines the physical location of an asset in Data Center 4:

- Enter a name for the annotation, such as "Location"
- Enter a description of what the annotation is describing, such as "Physical location is Data Center 4"
- Enter the 'type' of annotation it is, such as "Text".

Manually assigning annotations to assets

Assigning annotations to assets helps you sort, group, and report on assets in ways that are relevant to your business. Although you can assign annotations to assets of a particular type automatically using annotation rules, you can assign annotations to an individual asset by using its asset page.

Before you begin

- You must have created the annotation you want to assign.

Steps

1. Log in to your Cloud Insights environment.
2. Locate the asset to which you want to apply the annotation.
 - You can locate assets by querying, choosing from a dashboard widget, or search. When you have located the asset you want, click the link to open the asset's landing page.
3. On the asset page, in the User Data section, click **+ Annotation**.
4. The Add Annotation dialog box displays.
5. Select an annotation from the list.

6. Click **Value** and do either of the following, depending on type of annotation you selected:

- If the annotation type is list, date, or Boolean, select a value from the list.
- If the annotation type is text, type a value.

7. Click **Save**.

If you want to change the value of the annotation after you assign it, click the annotation field and select a different value.

If the annotation is of list type for which the *Add new values on the fly* option is selected, you can type a new value in addition to selecting an existing value.

Assigning annotations using annotation rules

To automatically assign annotations to assets based on criteria that you define, you configure annotation rules. Cloud Insights assigns the annotations to assets based on these rules. Cloud Insights also provides two default annotation rules, which you can modify to suit your needs or remove if you do not want to use them.

Creating annotation rules

As an alternative to manually applying annotations to individual assets, you can automatically apply annotations to multiple assets using annotation rules. Annotations set manually on an individual asset pages take precedence over rule-based annotations when Insight evaluates the annotation rules.

Before you begin

You must have created a query for the annotation rule.

About this task

Although you can edit the annotation types while you are creating the rules, you should have defined the types ahead of time.

Steps

1. Click **Manage > Annotation rules**

The Annotation Rules page displays the list of existing annotation rules.

2. Click **+ Add**.

3. Do the following:

- a. In the **Name** box, enter a unique name that describes the rule.

This name will appear in the Annotation Rules page.

- b. Click **Query** and select the query that is used to apply the annotation to assets.

- c. Click **Annotation** and select the annotation you want to apply.

- d. Click **Value** and select a value for the annotation.

For example, if you choose Birthday as the annotation, you specify a date for the value.

- e. Click **Save**

- f. Click **Run all rules** if you want to run all the rules immediately; otherwise, the rules are run at a regularly scheduled interval.

Creating annotation rules

You can use annotation rules to automatically apply annotations to multiple assets based on criteria that you define. Cloud Insights assigns the annotations to assets based on these rules. Annotations set manually on an individual asset pages take precedence over rule-based annotations when Cloud Insight evaluates the annotation rules.

Before you begin

You must have created a query for the annotation rule.

Steps

1. In the Cloud Insights menu click **Manage > Annotation rules**.
2. Click **+ Rule** to add a new annotation rule.

The Add Rule dialog is displayed.

3. Do the following:
 - a. In the **Name** box, enter a unique name that describes the rule.

The name appears in the Annotation Rules page.

- b. Click **Query** and select the query that Cloud Insights uses to identify the assets the annotation applies to.
- c. Click **Annotation** and select the annotation you want to apply.
- d. Click **Value** and select a value for the annotation.

For example, if you choose Birthday as the annotation, you specify a date for the value.

- e. Click **Save**
- f. Click **Run all rules** if you want to run all the rules immediately; otherwise, the rules are run at a regularly scheduled interval.



In a large Cloud Insights environment, you may notice that running annotation rules seems to take a while to complete. This is because the indexer runs first and must complete prior to running the rules. The indexer is what gives Cloud Insights the ability to search or filter for new or updated objects and counters in your data. The rules engine waits until the indexer completes its update before applying the rules.

Modifying annotation rules

You can modify an annotation rule to change the rule's name, its annotation, the annotation's value, or the query associated with the rule.

Steps

1. In the Cloud Insights menu, Click **Manage > Annotation rules**.

The Annotation Rules page displays the list of existing annotation rules.

2. Locate the Annotation Rule you want to modify.

You can filter the annotation rules by entering a value in the filter box or click a page number to browse through the annotation rules by page.

3. Click the menu icon for the rule that you want to modify.
4. Click **Edit**

The Edit Rule dialog is displayed.

5. Modify the annotation rule's name, annotation, value, or query.

Changing the Order of Rules

Annotation rules are processed from the top of the rules list to the bottom. To change the order in which a rule is processed, do the following:

Steps

1. Click on the menu icon for the rule you want to move.
2. Click **Move Up** or **Move Down** as needed until the rule appears in the location you want.

Note that when running multiple rules that update the same annotation on an asset, the first rule (as run from the top down) applies the annotation and updates the asset, then the second rule applies but doesn't change any annotation that was already set by the previous rule.

Deleting annotation rules

You might want to delete annotation rules that are no longer used.

Steps

1. In the Cloud Insights menu, Click **Manage > Annotation rules**.

The Annotation Rules page displays the list of existing annotation rules.

2. Locate the Annotation Rule you want to delete.

You can filter the annotation rules by entering a value in the filter box or click a page number to browse through the annotation rules by page.

3. Click the menu icon for the rule that you want to delete.
4. Click **Delete**

A confirmation message is displayed, prompting whether you want to delete the rule.

5. Click **OK**

Importing Annotations

Cloud Insights includes an API for importing annotations or applications from a CSV file, and assigning them to objects you specify.



The Cloud Insights API is available in **Cloud Insights Premium Edition**.

Importing

The **Admin > API Access** links contain [documentation](#) for the **Assets/Import** API. This documentation contains information on the .CSV file format.

ASSETS.import

PUT /assets/import Import assets from a CSV file.

Import annotations and applications from the given CSV file. The format of the CSV file is following:

```
, <Annotation Type> [, Annotation Type ...] [, Application] [, Tenant] [, Line_of_Business] [, Business_Unit] [, Project]
<Object Type Value 1>, <Object Name or Key 1>, <Annotation Value> [, Annotation Value ...] [, Application] [, Tenant] [, Line_of_Business] [, Business_Unit] [, Project]
<Object Type Value 2>, <Object Name or Key 2>, <Annotation Value> [, Annotation Value ...] [, Application] [, Tenant] [, Line_of_Business] [, Business_Unit] [, Project]
<Object Type Value 3>, <Object Name or Key 3>, <Annotation Value> [, Annotation Value ...] [, Application] [, Tenant] [, Line_of_Business] [, Business_Unit] [, Project]
...
<Object Type Value N>, <Object Name or Key N>, <Annotation Value> [, Annotation Value ...] [, Application] [, Tenant] [, Line_of_Business] [, Business_Unit] [, Project]
```

.CSV File Format

The general format of the CSV file is as follows. The first line of the file defines the import fields and specifies the order of the fields. This is followed by separate lines for each annotation or application. You do not need to define every field. However, the subsequent annotation lines must follow the same order as the definition line.

```
[Object Type] , [Object Name or ID] , Annotation Type [, Annotation Type,
...] [, Application] [, Tenant] [, Line_of_Business] [, Business_Unit] [, Project]
```

See the API Documentation for examples of .CSV files.

You can import and assign annotations from a .CSV file from within the API swagger itself. Simply choose the file to use and click the *Execute* button:

Parameters Cancel

No parameters

Request body multipart/form-data

CSV file to import

data Choose File No file chosen
string(\$binary)

Execute Clear

Responses

Import Behavior

During the import operation, data is added, merged, or replaced, depending on the objects and object types that are being imported. While importing, keep in mind the following behaviors.

- Adds an annotation or application if none exists with the same name in the target system.

- Merges an annotation if the annotation type is a list, and an annotation with the same name exists in the target system.
- Replaces an annotation if the annotation type is anything other than a list, and an annotation with the same name exists in the target system.

Note: If an annotation with the same name but with a different type exists in the target system, the import fails. If objects depend on the failed annotation, those objects may show incorrect or unwanted information. You must check all annotation dependencies after the import operation is complete.

- If an annotation value is empty then that annotation is removed from the object. Inherited annotations are not affected.
- Date type annotation values must be passed in as unix time in milliseconds.
- When annotating volumes or internal volumes, the object name is a combination of storage name and volume name using the "->" separator. For example: <Storage Name>-><Volume Name>
- If an object name contains a comma, the whole name must be in double quotes. For example: "NetApp1,NetApp2"->023F
- When attaching annotating to storages, switches, and ports, the 'Application' column will be ignored.
- Tenant, Line_Of_Business, Business_Unit, and/or Project makes a business entity. As with all business entities, any of the values can be empty.

The following object types can be annotated.

OBJECT TYPE	NAME OR KEY
Host	id-><id> or <Name> or <IP>
VM	id-><id> or <Name>
StoragePool	id-><id> or <Storage Name>-><Storage Pool Name>
InternalVolume	id-><id> or <Storage Name>-><Internal Volume Name>
Volume	id-><id> or <Storage Name>-><Volume Name>
Storage	id-><id> or <Name> or <IP>
Switch	id-><id> or <Name> or <IP>
Port	id-><id> or <WWN>
Qtree	id-><id> or <Storage Name>-><Internal Volume Name>-><Qtree Name>
Share	id-><id> or <Storage Name>-><Internal Volume Name>-><Share Name>-><Protocol>[-><Qtree Name (optional in case of default Qtree)>]

Working with Applications

Tracking asset usage by application

Understanding the applications used in your company's environment helps you to keep track of asset usage and cost.

Before you can track data associated with the applications running in your environment, you must first define those applications and associate them with the appropriate assets. You can associate applications with the following assets: hosts, virtual machines, volumes, internal volumes, qtrees, shares, and hypervisors.

This topic provides an example of tracking the usage of virtual machines that the Marketing Team uses for its Exchange email.

You might want to create a table similar to the following to identify applications used in your environment and note the group or business unit using each applications.

Tenant	Line of Business	Business Unit	Project	Applications
NetApp	Data Storage	Legal	Patents	Oracle Identity Manager, Oracle On Demand, PatentWiz
NetApp	Data Storage	Marketing	Sales Events	Exchange, Oracle Shared DataBase, BlastOff Event Planner

The table shows that that Marketing Team uses the Exchange application. We want to track their virtual machine utilization for Exchange, so that we can predict when we will need to add more storage. We can associate the Exchange application with all of Marketing's virtual machines:

1. Create an application named *Exchange*
2. Go to **Queries > +New Query** to create a new query for virtual machines (or select an existing VM query, if applicable).

Assuming the Marketing team's VMs all have a name containing the string “mkt”, create your query to filter VM name for “mkt”.

3. Select the VMs.
4. Associate the VMs with the *Exchange* application using **Bulk Actions > Add Applications**.
5. Select the desired application and click **Save**.
6. When finished, **Save** the query.

Creating Applications

To track data associated with specific applications running in your environment, you can define the applications in Cloud Insights.

Before you begin

If you want to associate the application with a business entity, you must create the business entity before you define the application.

About this task

Cloud Insights allows you to track data from assets associated with applications for things like usage or cost reporting.

Steps

1. In the Cloud Insights menu, click **Manage > Applications**.

The Add Application dialog box displays.

2. Enter a unique name for the application.
3. Select a priority for the application.
4. Click **Save**.

After defining an application, it can be assigned to assets.

Assigning applications to assets

This procedure assigns the application to a host as an example. You can assign host, virtual machine, volume, or internal volumes to an application.

Steps

1. Locate the asset to which you want to assign to the application:
2. Click **Queries > +New Query** and search for Host.
3. Click the check box on the left of the Host you want to associate with the application.
4. Click **Bulk Actions > Add Application**.
5. Select the Application you are assigning the asset to.

Any new applications you assign override any applications on the asset that were derived from another asset. For example, volumes inherit applications from hosts, and when new applications are assigned to a volume, the new application takes precedence over the derived application.

 For environments with large amounts of related assets, inheritance of application assignments to those assets could take several minutes. Please allow more time for inheritance to occur if you have many related assets.

After you finish

After assigning the host to the application you can assign the remaining assets to the application. To access the landing page for the application, click **Manage > Application** and select the application you created.

Monitors and Alerts

Alerting with Monitors

You create monitors to set thresholds that trigger alerts to notify you about issues related to the resources in your network. For example, you can create a monitor to alert for *node write latency* for any of a multitude of protocols.

Monitors and Alerting is available in all Cloud Insights Editions, however, Basic Edition is subject to the following:

* You may only have up to five custom monitors active at a time. Any monitors beyond five will be created in or moved to *Paused* state.

* VMDK, Virtual Machine, Host, and DataStore metrics monitors are not supported. If you have monitors created for these metrics, they will be paused and cannot be resumed when downgrading to Basic Edition.

Monitors allow you to set thresholds on metrics generated by "infrastructure" objects such as storage, VM, EC2, and ports, as well as for "integration" data such as those collected for Kubernetes, ONTAP advanced metrics, and Telegraf plugins. These *metric* monitors alert you when warning-level or critical-level thresholds are crossed.

You can also create monitors to trigger warning-, critical-, or informational-level alerts when specified *log events* are detected.

Cloud Insights provides a number of [System-Defined Monitors](#) as well, based on your environment.

Security Best Practice

Cloud Insights alerts are designed to highlight data points and trends in your environment, and Cloud Insights allows you to enter any valid email address as an alert recipient. If you are working in a secure environment, be especially mindful of who is receiving the notification or otherwise has access to the alert.

Metric or Log Monitor?

1. From the Cloud Insights menu, click **Alerts > Manage Monitors**

The Monitors list page is displayed, showing currently configured monitors.

2. To modify an existing monitor, click the monitor name in the list.
3. To add a monitor, Click **+ Monitor**.

Metric Monitor

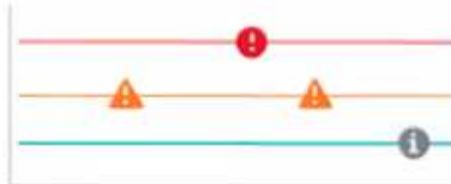
Set the high and low parameters that will trigger an alert if exceeded



Use when you know the upper and lower operating range

Log Monitor

Monitor logs and configure alerts



Use when you want to trigger alerts in response to log activity

When you add a new monitor, you are prompted to create a Metric Monitor or a Log Monitor.

- *Metric* monitors alert on infrastructure- or performance-related triggers
- *Log* monitors alert on log-related activity

After you choose your monitor type, the Monitor Configuration dialog is displayed. Configuration varies depending on which type of monitor you are creating.

Metric Monitor

1. In the drop-down, search for and choose an object type and metric to monitor.

You can set filters to narrow down which object attributes or metrics to monitor.

1 Select a metric to monitor

The screenshot shows a user interface for selecting a metric. At the top, there is a search bar containing the text "netapp_ontap.aggregate.cp_reads". Below the search bar are three buttons: "Filter By", "Group", and "Unit Display". To the right of these buttons is a blue "+" button. A dropdown menu is open, showing a list of metrics under the heading "Metrics". The metrics listed are: cp_read_blocks, cp_reads, data_compaction_space_saved, data_compaction_space_saved_percent, and size_total. The "cp_reads" metric is highlighted.

When working with integration data (Kubernetes, ONTAP Advanced Data, etc.), metric filtering removes the individual/unmatched data points from the plotted data series, unlike infrastructure data (storage, VM, ports etc.) where filters work on the aggregated value of the data series and potentially remove the entire object from the chart.



To create a multi-condition monitor (e.g., IOPS > X and latency > Y), define the first condition as a threshold and the second condition as a filter.

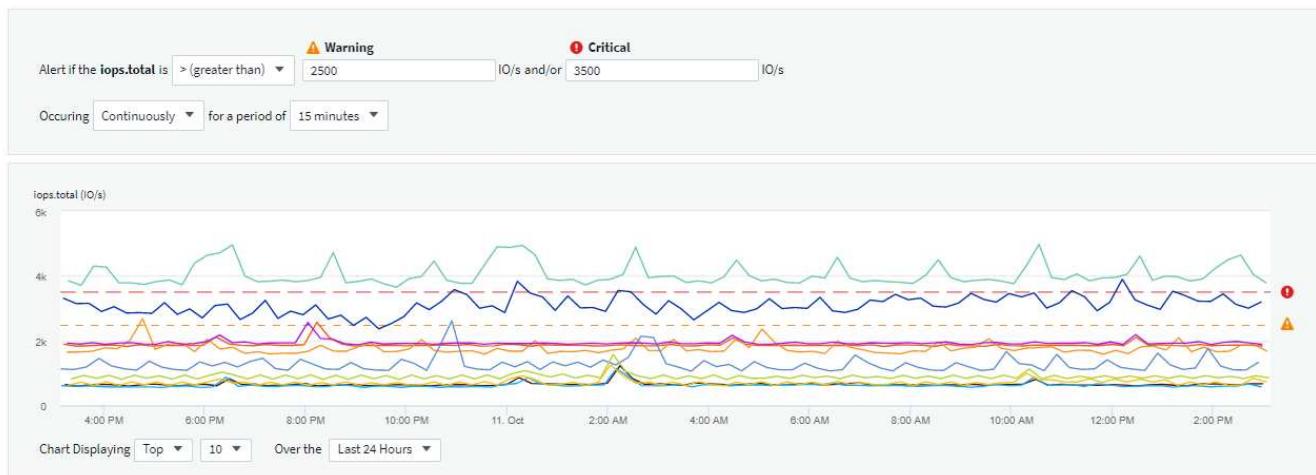
Define the Conditions of the Monitor.

1. After choosing the object and metric to monitor, set the Warning-level and/or Critical-level thresholds.
2. For the *Warning* level, enter 200 for our example. The dashed line indicating this *Warning* level displays in the example graph.
3. For the *Critical* level, enter 400. The dashed line indicating this *Critical* level displays in the example graph.

The graph displays historical data. The *Warning* and *Critical* level lines on the graph are a visual representation of the Monitor, so you can easily see when the Monitor might trigger an alert in each case.

4. For the occurrence interval, choose *Continuously* for a period of *15 Minutes*.

You can choose to trigger an alert the moment a threshold is breached, or wait until the threshold has been in continuous breach for a period of time. In our example, we do not want to be alerted every time the Total IOPS peaks above the *Warning* or *Critical* level, but only when a monitored object continuously exceeds one of these levels for at least 15 minutes.



Log Monitor

When creating a **Log monitor**, first choose which log to monitor from the available log list. You can then filter based on the available attributes as above. You can also choose one or more "Group By" attributes.



The Log Monitor filter cannot be empty.

Define the alert Behavior

You can create the monitor to alert with a severity level of *Critical*, *Warning*, or *Informational*, when the conditions you defined above occur once (i.e. immediately), or wait to alert until the conditions occur 2 times or more.

Define the alert resolution behavior

You can choose how a log monitor alert is resolved. You are presented with three choices:

- Resolve instantly
- Purge after the data retention period (please refer to the Editions Page for details). Note that the Monitor has no resolution condition by definition, so an Alert will stay *active* and suppress all subsequent alerts generated by this monitor, until the data retention period has passed.
- Resolve based on log entry: Resolve alert when the log line is discovered as outlined in the following definition, or purge after the data retention period

Define alert resolution

- Resolve instantly
 Purge after the data retention period (please refer to the [Editions Page](#) for details)
 Resolve based on log entry: Resolve alert when the log line is discovered as outlined in the following definition, or purge after the data retention period

Log Source [logs.netapp.ems](#)

Filter By [+](#) [?](#)

Group By [All](#)

///

- * **Resolve instantly:** The alert is immediately resolved with no further action needed
- * **Resolve based on time:** The alert is resolved after the specified time has passed
- * **Resolve based on log entry:** The alert is resolved when a subsequent log activity has occurred. For example, when an object is logged as "available".

- Resolve instantly
- Resolve based on time
- Resolve based on log entry

Log Source logs.netapp.ems ▾

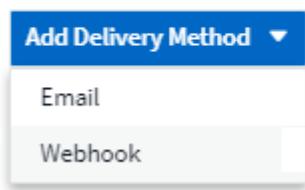
Filter By ems.ems_message_type "object.store.available" X X ▾ X +

///

Select notification type and recipients

In the *Set up team notification(s)* section, you can choose whether to alert your team via email or Webhook.

3 Set up team notification(s) (alert your team via email, or Webhook)



Alerting via Email:

Specify the email recipients for alert notifications. If desired, you can choose different recipients for warning or critical alerts.

3 Set up team notification(s)

<input checked="" type="checkbox"/> Email	Notify team on	Add Recipients (Required)
	Critical, Resolved	<input type="text" value="user_1@email.com"/> <input type="button" value="X"/>
	<input checked="" type="checkbox"/> Critical	
	<input type="checkbox"/> Warning	
	<input checked="" type="checkbox"/> Resolved	
<input checked="" type="checkbox"/> Email	Notify team on	Add Recipients (Required)
	Warning	<input type="text" value="user_3@email.com"/> <input type="button" value="X"/>

Alerting via Webhook:

Specify the webhook(s) for alert notifications. If desired, you can choose different webhooks for warning or critical alerts.

3 Set up team notification(s) (alert your team via email, or Webhook)

By Webhook	Notify team on	Slack	Use Webhook(s)
	Critical		<input type="text" value="Slack"/> <input type="button" value="X"/> <input type="text" value="Teams"/> <input type="button" value="X"/>
	Resolved		<input type="text" value="Slack"/> <input type="button" value="X"/> <input type="text" value="Teams"/> <input type="button" value="X"/>
	Warning		<input type="text" value="Slack"/> <input type="button" value="X"/> <input type="text" value="Teams"/> <input type="button" value="X"/>

 ONTAP Data Collector notifications take precedence over any specific Monitor notifications that are relevant to the cluster/data collector. The recipient list you set for the Data Collector itself will receive the data collector alerts. If there are no active data collector alerts, then monitor-generated alerts will be sent to specific monitor recipients.

Setting Corrective Actions or Additional Information

You can add an optional description as well as additional insights and/or corrective actions by filling in the **Add an Alert Description** section. The description can be up to 1024 characters and will be sent with the alert. The insights/corrective action field can be up to 67,000 characters and will be displayed in the summary section of the alert landing page.

In these fields you can provide notes, links, or steps to take to correct or otherwise address the alert.

4 Add an alert description (optional)

Add a description	Enter a description that will be sent with this alert (1024 character limit)
Add insights and corrective actions	Enter a url or details about the suggested actions to fix the issue raised by the alert

Save your Monitor

1. If desired, you can add a description of the monitor.
2. Give the Monitor a meaningful name and click **Save**.

Your new monitor is added to the list of active Monitors.

Monitor List

The Monitor page lists the currently configured monitors, showing the following:

- Monitor Name
- Status
- Object/metric being monitored
- Conditions of the Monitor

You can choose to temporarily pause monitoring of an object type by clicking the menu to the right of the monitor and selecting **Pause**. When you are ready to resume monitoring, click **Resume**.

You can copy a monitor by selecting **Duplicate** from the menu. You can then modify the new monitor and change the object/metric, filter, conditions, email recipients, etc.

If a monitor is no longer needed, you can delete it by selecting **Delete** from the menu.

Monitor Groups

Grouping allows you to view and manage related monitors. For example, you can have a monitor group dedicated to the storage in your environment, or monitors relevant to a certain recipient list.

The screenshot shows a user interface for managing monitor groups. At the top left is the title "Monitor Groups (5)". To the right are two small blue icons: a plus sign (+) and a back arrow. Below the title is a search bar with a magnifying glass icon and the placeholder text "Search groups...". The main area contains a list of groups, each with a name, a count in parentheses, and three vertical dots for additional actions. The groups listed are: "All Monitors (5)", "Custom Monitors (5)", "Agent Monitors (3)", and "ONTAP Aggregate Monitors (2)".

The following monitor groups are shown. The number of monitors contained in a group is shown next to the group name.

- **All Monitors** lists all monitors.
- **Custom Monitors** lists all user-created monitors.
- **Suspended Monitors** will list any system monitors that have been suspended by Cloud Insights.
- Cloud Insights will also show a number of **System Monitor Groups**, which will list one or more groups of [system-defined monitors](#), including ONTAP Infrastructure and Workload monitors.



Custom monitors can be paused, resumed, deleted, or moved to another group. System-defined monitors can be paused and resumed but can not be deleted or moved.

Suspended Monitors

This group will only be shown if Cloud Insights has suspended one or more monitors. A monitor may be suspended if it is generating excessive or continuous alerts. If the monitor is a custom monitor, modify the conditions to prevent the continuous alerting, and then resume the monitor. The monitor will be removed from the Suspended Monitors group when the issue causing the suspension is resolved.

System-Defined Monitors

These groups will show monitors provided by Cloud Insights, as long as your environment contains the devices and/or log availability required by the monitors.

System-Defined monitors cannot be modified, moved to another group, or deleted. However, you can duplicate a system monitor and modify or move the duplicate.

System monitors may include monitors for ONTAP Infrastructure (storage, volume, etc.) or Workloads (i.e. log monitors), or other groups. NetApp is constantly evaluating customer need and product functionality, and will update or add to system monitors and groups as needed.

Custom Monitor Groups

You can create your own groups to contain monitors based on your needs. For example, you may want a group for all of your storage-related monitors.

To create a new custom monitor group, click the "+" **Create New Monitor Group** button. Enter a name for the group and click **Create Group**. An empty group is created with that name.

To add monitors to the group, go to the *All Monitors* group (recommended) and do one of the following:

- To add a single monitor, click the menu to the right of the monitor and select *Add to Group*. Choose the group to which to add the monitor.
- Click on the monitor name to open the monitor's edit view, and select a group in the *Associate to a monitor group* section.

5 Associate to a monitor group (optional)

ONTAP Monitors



Remove monitors by clicking on a group and selecting *Remove from Group* from the menu. You can not remove monitors from the *All Monitors* or *Custom Monitors* group. To delete a monitor from these groups, you must delete the monitor itself.



Removing a monitor from a group does not delete the monitor from Cloud Insights. To completely remove a monitor, select the monitor and click *Delete*. This also removes it from the group to which it belonged and it is no longer available to any user.

You can also move a monitor to a different group in the same manner, selecting *Move to Group*.

To pause or resume all monitors in a group at once, select the menu for the group and click *Pause* or *Resume*.

Use the same menu to rename or delete a group. Deleting a group does not delete the monitors from Cloud Insights; they are still available in *All Monitors*.

The screenshot shows the Cloud Insights interface for managing monitor groups. At the top, there is a header with a search bar containing "Agent Monitors" and a clear button (X). Below the header, there is a list of monitor groups:

- Monitor Groups (3)**: Includes a blue "+" button and a blue square button with a white arrow.
- All Monitors (4)**: This group is currently selected, indicated by a blue border around its name.
- Custom Monitors (4)**
- Agent Monitors (3)**: This group has a blue vertical ellipsis menu button to its right, which is expanded to show the following options:
 - Pause
 - Resume
 - Rename
 - Delete

System-Defined Monitors

Cloud Insights includes a number of system-defined monitors for both metrics and logs. The system monitors available are dependent on the data collectors present in your environment. Because of that, the monitors available in Cloud Insights may change as data collectors are added or their configurations changed.

View the [System-Defined Monitors](#) page for descriptions of monitors included with Cloud Insights.

More Information

- [Viewing and Dismissing Alerts](#)

Viewing and Managing Alerts from Monitors

Cloud Insights displays alerts when [monitored thresholds](#) are exceeded.



Monitors and Alerting is available in Cloud Insights Standard Edition and higher.

Viewing and Managing Alerts

To view and manage alerts, do the following.

1. Navigate to the [Alerts > All Alerts](#) page.
2. A list of up to the most recent 1,000 alerts is displayed. You can sort this list on any field by clicking the column header for the field. The list displays the following information. Note that not all of these columns are displayed by default. You can select columns to display by clicking on the "gear" icon :
 - **Alert ID:** System-generated unique alert ID
 - **Triggered Time:** The time at which the relevant Monitor triggered the alert
 - **Current Severity** (Active alerts tab): The current severity of the active alert
 - **Top Severity** (Resolved alerts tab): The maximum severity of the alert before it was resolved
 - **Monitor:** The monitor configured to trigger the alert
 - **Triggered On:** The object on which the monitored threshold was breached
 - **Status:** Current alert status, *New* or *In Process*
 - **Active Status:** *Active* or *Resolved*
 - **Condition:** The threshold condition that triggered the alert
 - **Metric:** The object's metric on which the monitored threshold was breached
 - **Monitor Status:** Current status of the monitor that triggered the alert
 - **Has Corrective Action:** The alert has suggested corrective actions. Open the alert page to view these.

You can manage an alert by clicking the menu to the right of the alert and choosing one of the following:

- **In Process** to indicate that the alert is under investigation or otherwise needs to be kept open
- **Dismiss** to remove the alert from the list of active alerts.

You can manage multiple alerts by selecting the checkbox to the left of each Alert and clicking *Change Selected Alerts Status*.

Clicking on an Alert ID opens the Alert Detail Page.

Alert Detail Page

The Alert Detail Page provides additional detail about the alert, including a *Summary*, an *Expert View* showing graphs related to the object's data, any *Related Assets*, and *Comments* entered by alert investigators.

Alert Summary

Monitor:	Metric:
Volume Total Data	netapp_ontap.workload_volume.total_data
Triggered On:	Condition:
cluster_name: tawny aggr_name: Multiple_Values	Average total_data is > (greater than) 0m and/or 0m all the time in 2-hour window.
Duration / Time Triggered:	Filters Applied:
1d 6h / Jun 9, 2020 2:22 AM	cluster_name: Any
Top Severity:	Status:
Critical	New

Expert View

total_data (m)

Display Metrics ▾

Related Alerts

1 item found

Alert ID	Active Status	Triggered Time ↓	Top Severity	Monitor	Triggered On	Status
AL-46769	Resolved	a day ago Jun 9, 2020 2:22 AM	Critical	Volume Total Data	cluster_name: tawny aggr_name: Multiple_Values	New

Comments

There are no comments yet on this alert.

+ Comment

Alerts When Data Is Missing

In a realtime system such as Cloud Insights, to trigger the analysis of a Monitor to decide if an Alert should be generated, we rely on one of two things:

- the next datapoint to arrive
- a timer to fire when there is no datapoint and you have waited long enough

As is the case with slow data arrival—or no data arrival—the timer mechanism needs to take over as the data arrival rate is insufficient to trigger alerts in "real time." So the question typically becomes "How long do I wait before I close the analysis window and look at what I have?" If you wait too long then you are not generating the alerts fast enough to be useful.

If you have a Monitor with a 30-minute window that notices that a condition is violated by the last data point before a long-term loss-of-data, an Alert will be generated because the Monitor received no other information

to use to confirm a recovery of the metric or notice that the condition persisted.

"Permanently Active" Alerts

It is possible to configure a monitor in such a way for the condition to **always** exist on the monitored object—for example, IOPS > 1 or latency > 0. These are often created as 'test' monitors and then forgotten. Such monitors create alerts that stay permanently open on the constituent objects, which can cause system stress and stability issues over time.

To prevent this, Cloud Insights will automatically close any "permanently active" alert after 7 days. Note that the underlying monitor conditions may (probably will) continue to exist, causing a new alert to be issued almost immediately, but this closing of "always active" alerts alleviates some of the system stress that can otherwise occur.

Configuring Email Notifications

You can configure an email list for subscription-related notifications, as well as a global email list of recipients for notification of performance policy threshold violations.

To configure notification email recipient settings, go to the **Admin > Notifications** page and select the *Email* tab.

Subscription Notification Recipients

Send subscription related notifications to the following:

- All Account Owners
- All Monitor & Optimize Administrators
- Additional Email Addresses

X

Save

Global Monitor Notification Recipients

Default email recipients for monitor related notifications:

- All Account Owners
- All Monitor & Optimize Administrators
- Additional Email Addresses

Save

Subscription Notification Recipients

To configure recipients for subscription-related event notifications, go to the "Subscription Notification Recipients" section.

You can choose to have email notifications sent for subscription-related events to any or all of the following recipients:

- All Account Owners
- All *Monitor & Optimize* Administrators

- Additional Email Addresses that you specify

The following are examples of the types of notifications that might be sent, and user actions you can take.

Notification:	User Action:
Trial or subscription has been updated	Review subscription details on the Subscription page
Subscription will expire in 90 days Subscription will expire in 30 days	No action needed if “Auto Renewal” is enabled Contact NetApp sales to renew the subscription
Trial ends in 2 days	Renew trial from the Subscription page. You can renew a trial one time. Contact NetApp sales to purchase a subscription
Trial or subscription has expired Account will stop collecting data in 48 hours Account will be deleted after 48 hours	Contact NetApp sales to purchase a subscription

Global Recipient List for Alerts

Email notifications of alerts are sent to the alert recipient list for every action on the alert. You can choose to send alert notifications to a global recipient list.

To configure global alert recipients, choose the desired recipients in the **Global Monitor Notification Recipients** section.

You can always override the global recipients list for an individual monitor when creating or modifying the monitor.

 ONTAP Data Collector notifications take precedence over any specific Monitor notifications that are relevant to the cluster/data collector. The recipient list you set for the Data Collector itself will receive the data collector alerts. If there are no active data collector alerts, then monitor-generated alerts will be sent to specific monitor recipients.

System Monitors

Cloud Insights includes a number of system-defined monitors for both metrics and logs. The system monitors available are dependent on the data collectors present in your environment. Because of that, the monitors available in Cloud Insights may change as data collectors are added or their configurations changed.

 Most System Monitors are in *Paused* state by default. Before resuming the monitor, you must ensure that *Advanced Counter Data Collection* and *Enable ONTAP EMS log collection* are enabled in the Data Collector. These options can be found in the ONTAP Data Collector under *Advanced Configuration*:

- Enable ONTAP EMS log collection
- Opt in for Advanced Counter Data Collection rollout.

Monitor Descriptions

System-defined monitors are comprised of pre-defined metrics and conditions, as well as default descriptions and corrective actions, which can not be modified. You *can* modify the notification recipient list for system-defined monitors. To view the metrics, conditions, description and corrective actions, or to modify the recipient list, open a system-defined monitor group and click the monitor name in the list.

System-defined monitor groups cannot be modified or removed.

The following system-defined monitors are available, in the noted groups.

- **ONTAP Infrastructure** includes monitors for infrastructure-related issues in ONTAP clusters.
- **ONTAP Workload Examples** includes monitors for workload-related issues.
- Monitors in both group default to *Paused* state.

Below are the system monitors currently included with Cloud Insights:

Metric Monitors

Monitor Name	Severity	Monitor Description	Corrective Action
Fiber Channel Port Utilization High	CRITICAL	Fiber Channel Protocol ports are used to receive and transfer the SAN traffic between the customer host system and the ONTAP LUNs. If the port utilization is high, then it will become a bottleneck and it will ultimately affect the performance of sensitive of Fiber Channel Protocol workloads....A warning alert indicates that planned action should be taken to balance network traffic....A critical alert indicates that service disruption is imminent and emergency measures should be taken to balance network traffic to ensure service continuity.	If critical threshold is breached, consider immediate actions to minimize service disruption: 1. Move workloads to another lower utilized FCP port. 2. Limit the traffic of certain LUNs only to essential work, either via QoS policies in ONTAP or host-side configuration to lighten the utilization of the FCP ports.... If warning threshold is breached, plan to take the following actions: 1. Configure more FCP ports to handle the data traffic so that the port utilization gets distributed among more ports. 2. Move workloads to another lower utilized FCP port. 3. Limit the traffic of certain LUNs only to essential work, either via QoS policies in ONTAP or host-side configuration to lighten the utilization of the FCP ports.

Lun Latency High	CRITICAL	<p>LUNs are objects that serve the I/O traffic often driven by performance sensitive applications such as databases. High LUN latencies means that the applications themselves might suffer and be unable to accomplish their tasks....A warning alert indicates that planned action should be taken to move the LUN to appropriate Node or Aggregate....A critical alert indicates that service disruption is imminent and emergency measures should be taken to ensure service continuity.</p> <p>Following are expected latencies based on media type - SSD up to 1-2 milliseconds; SAS up to 8-10 milliseconds, and SATA HDD 17-20 milliseconds</p>	<p>If critical threshold is breached, consider following actions to minimize service disruption:</p> <p>If the LUN or its volume has a QoS policy associated with it, then evaluate its threshold limits and validate if they are causing the LUN workload to get throttled....</p> <p>If warning threshold is breached, plan to take the following actions:</p> <ol style="list-style-type: none"> 1. If aggregate is also experiencing high utilization, move the LUN to another aggregate. 2. If the node is also experiencing high utilization, move the volume to another node or reduce the total workload of the node. 3. If the LUN or its volume has a QoS policy associated with it, evaluate its threshold limits and validate if they are causing the LUN workload to get throttled.
------------------	----------	---	---

Network Port Utilization High	CRITICAL	<p>Network ports are used to receive and transfer the NFS, CIFS, and iSCSI protocol traffic between the customer host systems and the ONTAP volumes. If the port utilization is high, then it becomes a bottleneck and it will ultimately affect the performance of NFS, CIFS and iSCSI workloads....A warning alert indicates that planned action should be taken to balance network traffic....A critical alert indicates that service disruption is imminent and emergency measures should be taken to balance network traffic to ensure service continuity.</p>	<p>If critical threshold is breached, consider following immediate actions to minimize service disruption:</p> <ol style="list-style-type: none"> 1. Limit the traffic of certain volumes only to essential work, either via QoS policies in ONTAP or host-side analysis to decrease the utilization of the network ports. 2. Configure one or more volumes to use another lower utilized network port.... <p>If warning threshold is breached, consider the following immediate actions:</p> <ol style="list-style-type: none"> 1. Configure more network ports to handle the data traffic so that the port utilization gets distributed among more ports. 2. Configure one or more volumes to use another lower utilized network port.
-------------------------------	----------	---	--

NVMe Namespace Latency High	CRITICAL	<p>NVMe Namespaces are objects that serve the I/O traffic that is driven by performance sensitive applications such as databases. High NVMe Namespaces latency means that the applications themselves may suffer and be unable to accomplish their tasks....A warning alert indicates that planned action should be taken to move the LUN to appropriate Node or Aggregate....A critical alert indicates that service disruption is imminent and emergency measures should be taken to ensure service continuity.</p>	<p>If critical threshold is breached, consider immediate actions to minimize service disruption:</p> <p>If the NVMe namespace or its volume has a QoS policy assigned to them, then evaluate its limit thresholds in case they are causing the NVMe namespace workload to get throttled....</p> <p>If warning threshold is breached, consider to take the following actions:</p> <ol style="list-style-type: none"> 1. If aggregate is also experiencing high utilization, move the LUN to another aggregate. 2. If the node is also experiencing high utilization, move the volume to another node or reduce the total workload of the node. 3. If the NVMe namespace or its volume has a QoS policy assigned to them, evaluate its limit thresholds in case they are causing the NVMe namespace workload to get throttled.
-----------------------------	----------	---	---

QTree Capacity Full	CRITICAL	<p>A qtree is a logically defined file system that can exist as a special subdirectory of the root directory within a volume. Each qtree has a default space quota or a quota defined by a quota policy to limit amount of data stored in the tree within the volume capacity....A warning alert indicates that planned action should be taken to increase the space....A critical alert indicates that service disruption is imminent and emergency measures should be taken to free up space to ensure service continuity.</p>	<p>If critical threshold is breached, consider immediate actions to minimize service disruption:</p> <ol style="list-style-type: none"> 1. Increase the space of the qtree in order to accommodate the growth. 2. Delete unwanted data to free up space.... <p>If warning threshold is breached, plan to take the following immediate actions:</p> <ol style="list-style-type: none"> 1. Increase the space of the qtree in order to accommodate the growth. 2. Delete unwanted data to free up space.
QTree Capacity Hard Limit	CRITICAL	<p>A qtree is a logically defined file system that can exist as a special subdirectory of the root directory within a volume. Each qtree has a space quota measured in KBytes that is used to store data in order to control the growth of user data in volume and not exceed its total capacity....A qtree maintains a soft storage capacity quota that provides alert to the user proactively before reaching the total capacity quota limit in the qtree and being unable to store data anymore. Monitoring the amount of data stored within a qtree ensures that the user receives uninterrupted data service.</p>	<p>If critical threshold is breached, consider following immediate actions to minimize service disruption:</p> <ol style="list-style-type: none"> 1. Increase the tree space quota in order to accommodate the growth 2. Instruct the user to delete unwanted data in the tree to free up space

QTree Capacity Soft Limit	WARNING	<p>A qtree is a logically defined file system that can exist as a special subdirectory of the root directory within a volume. Each qtree has a space quota measured in KBytes that it can use to store data in order to control the growth of user data in volume and not exceed its total capacity....A qtree maintains a soft storage capacity quota that provides alert to the user proactively before reaching the total capacity quota limit in the qtree and being unable to store data anymore. Monitoring the amount of data stored within a qtree ensures that the user receives uninterrupted data service.</p>	<p>If warning threshold is breached, consider the following immediate actions:</p> <ol style="list-style-type: none"> 1. Increase the tree space quota to accommodate the growth. 2. Instruct the user to delete unwanted data in the tree to free up space.
QTree Files Hard Limit	CRITICAL	<p>A qtree is a logically defined file system that can exist as a special subdirectory of the root directory within a volume. Each qtree has a quota of the number of files that it can contain to maintain a manageable file system size within the volume....A qtree maintains a hard file number quota beyond which new files in the tree are denied. Monitoring the number of files within a qtree ensures that the user receives uninterrupted data service.</p>	<p>If critical threshold is breached, consider immediate actions to minimize service disruption:</p> <ol style="list-style-type: none"> 1. Increase the file count quota for the qtree. 2. Delete unwanted files from the qtree file system.

QTree Files Soft Limit	WARNING	<p>A qtree is a logically defined file system that can exist as a special subdirectory of the root directory within a volume. Each qtree has a quota of the number of files that it can contain in order to maintain a manageable file system size within the volume....A qtree maintains a soft file number quota to provide alert to the user proactively before reaching the limit of files in the qtree and being unable to store any additional files. Monitoring the number of files within a qtree ensures that the user receives uninterrupted data service.</p>	<p>If warning threshold is breached, plan to take the following immediate actions:</p> <ol style="list-style-type: none"> 1. Increase the file count quota for the qtree. 2. Delete unwanted files from the qtree file system.
Snapshot Reserve Space Full	CRITICAL	<p>Storage capacity of a volume is necessary to store application and customer data. A portion of that space, called snapshot reserved space, is used to store snapshots which allow data to be protected locally. The more new and updated data stored in the ONTAP volume the more snapshot capacity is used and less snapshot storage capacity is available for future new or updated data. If the snapshot data capacity within a volume reaches the total snapshot reserve space, it might lead to the customer being unable to store new snapshot data and reduction in the level of protection for the data in the volume. Monitoring the volume used snapshot capacity ensures data services continuity.</p>	<p>If critical threshold is breached, consider immediate actions to minimize service disruption:</p> <ol style="list-style-type: none"> 1. Configure snapshots to use data space in the volume when the snapshot reserve is full. 2. Delete some older unwanted snapshots to free up space.... <p>If warning threshold is breached, plan to take the following immediate actions:</p> <ol style="list-style-type: none"> 1. Increase the snapshot reserve space within the volume to accommodate the growth. 2. Configure snapshots to use data space in the volume when the snapshot reserve is full.

Storage Capacity Limit	CRITICAL	<p>When a storage pool (aggregate) is filling up, I/O operations slow down and finally stop resulting in storage outage incident. A warning alert indicates that planned action should be taken soon to restore minimum free space. A critical alert indicates that service disruption is imminent and emergency measures should be taken to free up space to ensure service continuity.</p>	<p>If critical threshold is breached, immediately consider the following actions to minimize service disruption:</p> <ol style="list-style-type: none"> 1. Delete Snapshots on non-critical volumes. 2. Delete Volumes or LUNs that are non-essential workloads and that may be restored from off storage copies.....If warning threshold is breached, plan the following immediate actions: 1. Move one or more volumes to a different storage location. 2. Add more storage capacity. 3. Change storage efficiency settings or tier inactive data to cloud storage.
Storage Performance Limit	CRITICAL	<p>When a storage system reaches its performance limit, operations slow down, latency goes up and workloads and applications may start failing. ONTAP evaluates the storage pool utilization for workloads and estimates what percent of performance has been consumed....A warning alert indicates that planned action should be taken to reduce storage pool load to ensure that there will be enough storage pool performance left to service workload peaks....A critical alert indicates that a performance brownout is imminent and emergency measures should be taken to reduce storage pool load to ensure service continuity.</p>	<p>If critical threshold is breached, consider following immediate actions to minimize service disruption:</p> <ol style="list-style-type: none"> 1. Suspend scheduled tasks such as Snapshots or SnapMirror replication. 2. Idle non-essential workloads.... <p>If warning threshold is breached, take the following actions immediately:</p> <ol style="list-style-type: none"> 1. Move one or more workloads to a different storage location. 2. Add more storage nodes (AFF) or disk shelves(FAS) and redistribute workloads 3. Change workload characteristics(block size, application caching).

User Quota Capacity Hard Limit	CRITICAL	<p>ONTAP recognizes the users of Unix or Windows systems who have the rights to access volumes, files or directories within a volume. As a result, ONTAP allows the customers to configure storage capacity for their users or groups of users of their Linux or Windows systems. The user or group policy quota limits the amount of space the user can utilize for their own data....A hard limit of this quota allows notification of the user when the amount of capacity used within the volume is right before reaching the total capacity quota. Monitoring the amount of data stored within a user or group quota ensures that the user receives uninterrupted data service.</p>	<p>If critical threshold is breached, consider following immediate actions to minimize service disruption:</p> <ol style="list-style-type: none"> 1. Increase the space of the user or group quota in order to accommodate the growth. 2. Instruct the user or group to delete unwanted data to free up space.
--------------------------------	----------	--	--

User Quota Capacity Soft Limit	WARNING	<p>ONTAP recognizes the users of Unix or Windows systems that have the rights to access volumes, files or directories within a volume. As a result, ONTAP allows the customers to configure storage capacity for their users or groups of users of their Linux or Windows systems. The user or group policy quota limits the amount of space the user can utilize for their own data....A soft limit of this quota allows proactive notification to the user when the amount of capacity used within the volume is reaching the total capacity quota. Monitoring the amount of data stored within a user or group quota ensures that the user receives uninterrupted data service.</p>	<p>If warning threshold is breached, plan to take the following immediate actions:</p> <ol style="list-style-type: none"> 1. Increase the space of the user or group quota in order to accommodate the growth. 2. Delete unwanted data to free up space.
--------------------------------	---------	--	--

Volume Capacity Full	CRITICAL	<p>Storage capacity of a volume is necessary to store application and customer data. The more data stored in the ONTAP volume the less storage availability for future data. If the data storage capacity within a volume reaches the total storage capacity may lead to the customer being unable to store data due to lack of storage capacity. Monitoring the volume used storage capacity ensures data services continuity.</p>	<p>If critical threshold is breached, consider following immediate actions to minimize service disruption:</p> <ol style="list-style-type: none"> 1. Increase the space of the volume to accommodate the growth. 2. Delete unwanted data to free up space. 3. If snapshot copies occupy more space than the snapshot reserve, delete old Snapshots or enable Volume Snapshot Autodelete....If warning threshold is breached, plan to take the following immediate actions: <ol style="list-style-type: none"> 1. Increase the space of the volume in order to accommodate the growth 2. If snapshot copies occupy more space than the snapshot reserve, delete old Snapshots or enabling Volume Snapshot Autodelete.....
----------------------	----------	---	---

Volume Inodes Limit	CRITICAL	<p>Volumes that store files use index nodes (inode) to store file metadata. When a volume exhausts its inode allocation, no more files can be added to it....A warning alert indicates that planned action should be taken to increase the number of available inodes....A critical alert indicates that file limit exhaustion is imminent and emergency measures should be taken to free up inodes to ensure service continuity.</p>	<p>If critical threshold is breached, consider following immediate actions to minimize service disruption:</p> <ol style="list-style-type: none"> 1. Increase the inodes value for the volume. If the inodes value is already at the max value, then split the volume into two or more volumes because the file system has grown beyond the maximum size. 2. Use FlexGroup as it helps to accommodate large file systems.... <p>If warning threshold is breached, plan to take the following immediate actions:</p> <ol style="list-style-type: none"> 1. Increase the inodes value for the volume. If the inodes value is already at the max, then split the volume into two or more volumes because the file system has grown beyond the maximum size. 2. Use FlexGroup as it helps to accommodate large file systems
---------------------	----------	---	---

Volume Latency High	CRITICAL	<p>Volumes are objects that serve the I/O traffic often driven by performance sensitive applications including devOps applications, home directories, and databases. High volume latencies means that the applications themselves may suffer and be unable to accomplish their tasks.</p> <p>Monitoring volume latencies is critical to maintain application consistent performance.</p> <p>The following are expected latencies based on media type - SSD up to 1-2 milliseconds; SAS up to 8-10 milliseconds and SATA HDD 17-20 milliseconds.</p>	<p>If critical threshold is breached, consider following immediate actions to minimize service disruption:</p> <p>If the volume has a QoS policy assigned to it, evaluate its limit thresholds in case they are causing the volume workload to get throttled....</p> <p>If warning threshold is breached, consider the following immediate actions:</p> <ol style="list-style-type: none"> 1. If aggregate is also experiencing high utilization, move the volume to another aggregate. 2. If the volume has a QoS policy assigned to it, evaluate its limit thresholds in case they are causing the volume workload to get throttled. 3. If the node is also experiencing high utilization, move the volume to another node or reduce the total workload of the node.
Monitor Name	Severity	Monitor Description	Corrective Action

Node High Latency	WARNING / CRITICAL	<p>Node latency has reached the levels where it might affect the performance of the applications on the node. Lower node latency ensures consistent performance of the applications. The expected latencies based on media type are: SSD up to 1-2 milliseconds; SAS up to 8-10 milliseconds and SATA HDD 17-20 milliseconds.</p>	<p>If critical threshold is breached, then immediate actions should be taken to minimize service disruption:</p> <ol style="list-style-type: none"> 1. Suspend scheduled tasks, Snapshots or SnapMirror replication 2. Lower the demand of lower priority workloads via QoS limits 3. Inactivate non-essential workloads <p>Consider immediate actions when warning threshold is breached:</p> <ol style="list-style-type: none"> 1. Move one or more workloads to a different storage location 2. Lower the demand of lower priority workloads via QoS limits 3. Add more storage nodes (AFF) or disk shelves (FAS) and redistribute workloads 4. Change workload characteristics (block size, application caching etc)
-------------------	--------------------	---	---

Node Performance Limit	WARNING / CRITICAL	<p>Node performance utilization has reached the levels where it might affect the performance of the IOs and the applications supported by the node. Low node performance utilization ensures consistent performance of the applications.</p>	<p>Immediate actions should be taken to minimize service disruption if critical threshold is breached:</p> <ol style="list-style-type: none"> 1. Suspend scheduled tasks, Snapshots or SnapMirror replication 2. Lower the demand of lower priority workloads via QoS limits 3. Inactivate non-essential workloads <p>Consider the following actions if warning threshold is breached:</p> <ol style="list-style-type: none"> 1. Move one or more workloads to a different storage location 2. Lower the demand of lower priority workloads via QoS limits 3. Add more storage nodes (AFF) or disk shelves (FAS) and redistribute workloads 4. Change workload characteristics (block size, application caching etc)
------------------------	--------------------	--	---

Storage VM High Latency	WARNING / CRITICAL	<p>Storage VM (SVM) latency has reached the levels where it might affect the performance of the applications on the storage VM. Lower storage VM latency ensures consistent performance of the applications. The expected latencies based on media type are: SSD up to 1-2 milliseconds; SAS up to 8-10 milliseconds and SATA HDD 17-20 milliseconds.</p>	<p>If critical threshold is breached, then immediately evaluate the threshold limits for volumes of the storage VM with a QoS policy assigned, to verify whether they are causing the volume workloads to get throttled</p> <p>Consider following immediate actions when warning threshold is breached:</p> <ol style="list-style-type: none"> 1. If aggregate is also experiencing high utilization, move some volumes of the storage VM to another aggregate. 2. For volumes of the storage VM with a QoS policy assigned, evaluate the threshold limits if they are causing the volume workloads to get throttled 3. If the node is experiencing high utilization, move some volumes of the storage VM to another node or reduce the total workload of the node
User Quota Files Hard Limit	CRITICAL	<p>The number of files created within the volume has reached the critical limit and additional files cannot be created. Monitoring the number of files stored ensures that the user receives uninterrupted data service.</p>	<p>Immediate actions are required to minimize service disruption if critical threshold is breached....Consider taking following actions:</p> <ol style="list-style-type: none"> 1. Increase the file count quota for the specific user 2. Delete unwanted files to reduce the pressure on the files quota for the specific user

User Quota Files Soft Limit	WARNING	The number of files created within the volume has reached the threshold limit of the quota and is near to the critical limit. You cannot create additional files if quota reaches the critical limit. Monitoring the number of files stored by a user ensures that the user receives uninterrupted data service.	Consider immediate actions if warning threshold is breached: 1. Increase the file count quota for the specific user quota 2. Delete unwanted files to reduce the pressure on the files quota for the specific user
Volume Cache Miss Ratio	WARNING / CRITICAL	<p>Volume Cache Miss Ratio is the percentage of read requests from the client applications that are returned from the disk instead of being returned from the cache. This means that the volume has reached the set threshold.</p>	<p>If critical threshold is breached, then immediate actions should be taken to minimize service disruption:</p> <ol style="list-style-type: none"> 1. Move some workloads off of the node of the volume to reduce the IO load 2. If not already on the node of the volume, increase the WAFL cache by purchasing and adding a Flash Cache 3. Lower the demand of lower priority workloads on the same node via QoS limits <p>Consider immediate actions when warning threshold is breached:</p> <ol style="list-style-type: none"> 1. Move some workloads off of the node of the volume to reduce the IO load 2. If not already on the node of the volume, increase the WAFL cache by purchasing and adding a Flash Cache 3. Lower the demand of lower priority workloads on the same node via QoS limits 4. Change workload characteristics (block size, application caching etc)

Volume Qtree Quota Overcommit	WARNING / CRITICAL	<p>Volume Qtree Quota Overcommit specifies the percentage at which a volume is considered to be overcommitted by the qtree quotas. The set threshold for the qtree quota is reached for the volume. Monitoring the volume qtree quota overcommit ensures that the user receives uninterrupted data service.</p>	<p>If critical threshold is breached, then immediate actions should be taken to minimize service disruption:</p> <ol style="list-style-type: none"> 1. Increase the space of the volume 2. Delete unwanted data <p>When warning threshold is breached, then consider increasing the space of the volume.</p>
-------------------------------	--------------------	---	--

[Back to Top](#)

Log Monitors

Monitor Name	Severity	Description	Corrective Action
AWS Credentials Not Initialized	INFO	This event occurs when a module attempts to access Amazon Web Services (AWS) Identity and Access Management (IAM) role-based credentials from the cloud credentials thread before they are initialized.	Wait for the cloud credentials thread, as well as the system, to complete initialization.

Cloud Tier Unreachable	CRITICAL	<p>A storage node cannot connect to Cloud Tier object store API. Some data will be inaccessible.</p>	<p>If you use on-premises products, perform the following corrective actions: ...Verify that your intercluster LIF is online and functional by using the "network interface show" command....Check the network connectivity to the object store server by using the "ping" command over the destination node intercluster LIF....Ensure the following:...The configuration of your object store has not changed....The login and connectivity information is still valid....Contact NetApp technical support if the issue persists.</p> <p>If you use Cloud Volumes ONTAP, perform the following corrective actions: ...Ensure that the configuration of your object store has not changed.... Ensure that the login and connectivity information is still valid....Contact NetApp technical support if the issue persists.</p>
Disk Out of Service	INFO	<p>This event occurs when a disk is removed from service because it has been marked failed, is being sanitized, or has entered the Maintenance Center.</p>	<p>None.</p>

FlexGroup Constituent Full	CRITICAL	A constituent within a FlexGroup volume is full, which might cause a potential disruption of service. You can still create or expand files on the FlexGroup volume. However, none of the files that are stored on the constituent can be modified. As a result, you might see random out-of-space errors when you try to perform write operations on the FlexGroup volume.	It is recommended that you add capacity to the FlexGroup volume by using the "volume modify -files +X" command....Alternatively, delete files from the FlexGroup volume. However, it is difficult to determine which files have landed on the constituent.
Flexgroup Constituent Nearly Full	WARNING	A constituent within a FlexGroup volume is nearly out of space, which might cause a potential disruption of service. Files can be created and expanded. However, if the constituent runs out of space, you might not be able to append to or modify the files on the constituent.	It is recommended that you add capacity to the FlexGroup volume by using the "volume modify -files +X" command....Alternatively, delete files from the FlexGroup volume. However, it is difficult to determine which files have landed on the constituent.
FlexGroup Constituent Nearly Out of Inodes	WARNING	A constituent within a FlexGroup volume is almost out of inodes, which might cause a potential disruption of service. The constituent receives lesser create requests than average. This might impact the overall performance of the FlexGroup volume, because the requests are routed to constituents with more inodes.	It is recommended that you add capacity to the FlexGroup volume by using the "volume modify -files +X" command....Alternatively, delete files from the FlexGroup volume. However, it is difficult to determine which files have landed on the constituent.

FlexGroup Constituent Out of Inodes	CRITICAL	A constituent of a FlexGroup volume has run out of inodes, which might cause a potential disruption of service. You cannot create new files on this constituent. This might lead to an overall imbalanced distribution of content across the FlexGroup volume.	It is recommended that you add capacity to the FlexGroup volume by using the "volume modify -files +X" command....Alternatively, delete files from the FlexGroup volume. However, it is difficult to determine which files have landed on the constituent.
LUN Offline	INFO	This event occurs when a LUN is brought offline manually.	Bring the LUN back online.
Main Unit Fan Failed	WARNING	One or more main unit fans have failed. The system remains operational....However, if the condition persists for too long, the overtemperature might trigger an automatic shutdown.	Reseat the failed fans. If the error persists, replace them.
Main Unit Fan in Warning State	INFO	This event occurs when one or more main unit fans are in a warning state.	Replace the indicated fans to avoid overheating.
NVRAM Battery Low	WARNING	The NVRAM battery capacity is critically low. There might be a potential data loss if the battery runs out of power....Your system generates and transmits an AutoSupport or "call home" message to NetApp technical support and the configured destinations if it is configured to do so. The successful delivery of an AutoSupport message significantly improves problem determination and resolution.	Perform the following corrective actions:...View the battery's current status, capacity, and charging state by using the "system node environment sensors show" command....If the battery was replaced recently or the system was non-operational for an extended period of time, monitor the battery to verify that it is charging properly....Contact NetApp technical support if the battery runtime continues to decrease below critical levels, and the storage system shuts down automatically.

Service Processor Not Configured	WARNING	<p>This event occurs on a weekly basis, to remind you to configure the Service Processor (SP). The SP is a physical device that is incorporated into your system to provide remote access and remote management capabilities. You should configure the SP to use its full functionality.</p>	<p>Perform the following corrective actions:...Configure the SP by using the "system service-processor network modify" command....Optionally, obtain the MAC address of the SP by using the "system service-processor network show" command....Verify the SP network configuration by using the "system service-processor network show" command....Verify that the SP can send an AutoSupport email by using the "system service-processor autosupport invoke" command. NOTE: AutoSupport email hosts and recipients should be configured in ONTAP before you issue this command.</p>
Service Processor Offline	CRITICAL	<p>ONTAP is no longer receiving heartbeats from the Service Processor (SP), even though all the SP recovery actions have been taken. ONTAP cannot monitor the health of the hardware without the SP....The system will shut down to prevent hardware damage and data loss. Set up a panic alert to be notified immediately if the SP goes offline.</p>	<p>Power-cycle the system by performing the following actions:...Pull the controller out from the chassis....Push the controller back in....Turn the controller back on....If the problem persists, replace the controller module.</p>

Shelf Fans Failed	CRITICAL	The indicated cooling fan or fan module of the shelf has failed. The disks in the shelf might not receive enough cooling airflow, which might result in disk failure.	Perform the following corrective actions:...Verify that the fan module is fully seated and secured. NOTE: The fan is integrated into the power supply module in some disk shelves....If the issue persists, replace the fan module....If the issue still persists, contact NetApp technical support for assistance.
System Cannot Operate Due to Main Unit Fan Failure	CRITICAL	One or more main unit fans have failed, disrupting system operation. This might lead to a potential data loss.	Replace the failed fans.
Unassigned Disks	INFO	System has unassigned disks - capacity is being wasted and your system may have some misconfiguration or partial configuration change applied.	Perform the following corrective actions:...Determine which disks are unassigned by using the "disk show -n" command....Assign the disks to a system by using the "disk assign" command.
Antivirus Server Busy	WARNING	The antivirus server is too busy to accept any new scan requests.	If this message occurs frequently, ensure that there are enough antivirus servers to handle the virus scan load generated by the SVM.
AWS Credentials for IAM Role Expired	CRITICAL	Cloud Volume ONTAP has become inaccessible. The Identity and Access Management (IAM) role-based credentials have expired. The credentials are acquired from the Amazon Web Services (AWS) metadata server using the IAM role, and are used to sign API requests to Amazon Simple Storage Service (Amazon S3).	Perform the following:...Log in to the AWS EC2 Management Console....Navigate to the Instances page....Find the instance for the Cloud Volumes ONTAP deployment and check its health....Verify that the AWS IAM role associated with the instance is valid and has been granted proper privileges to the instance.

AWS Credentials for IAM Role Not Found	CRITICAL	The cloud credentials thread cannot acquire the Amazon Web Services (AWS) Identity and Access Management (IAM) role-based credentials from the AWS metadata server. The credentials are used to sign API requests to Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP has become inaccessible....	Perform the following:...Log in to the AWS EC2 Management Console....Navigate to the Instances page....Find the instance for the Cloud Volumes ONTAP deployment and check its health....Verify that the AWS IAM role associated with the instance is valid and has been granted proper privileges to the instance.
AWS Credentials for IAM Role Not Valid	CRITICAL	The Identity and Access Management (IAM) role-based credentials are not valid. The credentials are acquired from the Amazon Web Services (AWS) metadata server using the IAM role, and are used to sign API requests to Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP has become inaccessible.	Perform the following:...Log in to the AWS EC2 Management Console....Navigate to the Instances page....Find the instance for the Cloud Volumes ONTAP deployment and check its health....Verify that the AWS IAM role associated with the instance is valid and has been granted proper privileges to the instance.
AWS IAM Role Not Found	CRITICAL	The Identity and Access Management (IAM) roles thread cannot find an Amazon Web Services (AWS) IAM role on the AWS metadata server. The IAM role is required to acquire role-based credentials used to sign API requests to Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP has become inaccessible....	Perform the following:...Log in to the AWS EC2 Management Console....Navigate to the Instances page....Find the instance for the Cloud Volumes ONTAP deployment and check its health....Verify that the AWS IAM role associated with the instance is valid.

AWS IAM Role Not Valid	CRITICAL	The Amazon Web Services (AWS) Identity and Access Management (IAM) role on the AWS metadata server is not valid. The Cloud Volume ONTAP has become inaccessible....	Perform the following:...Log in to the AWS EC2 Management Console....Navigate to the Instances page....Find the instance for the Cloud Volumes ONTAP deployment and check its health....Verify that the AWS IAM role associated with the instance is valid and has been granted proper privileges to the instance.
AWS Metadata Server Connection Fail	CRITICAL	The Identity and Access Management (IAM) roles thread cannot establish a communication link with the Amazon Web Services (AWS) metadata server. Communication should be established to acquire the necessary AWS IAM role-based credentials used to sign API requests to Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP has become inaccessible....	Perform the following:...Log in to the AWS EC2 Management Console....Navigate to the Instances page....Find the instance for the Cloud Volumes ONTAP deployment and check its health....
FabricPool Space Usage Limit Nearly Reached	WARNING	The total cluster-wide FabricPool space usage of object stores from capacity-licensed providers has nearly reached the licensed limit.	Perform the following corrective actions:...Check the percentage of the licensed capacity used by each FabricPool storage tier by using the "storage aggregate object-store show-space" command....Delete Snapshot copies from volumes with the tiering policy "snapshot" or "backup" by using the "volume snapshot delete" command to clear up space....Install a new license on the cluster to increase the licensed capacity.

FabricPool Space Usage Limit Reached	CRITICAL	The total cluster-wide FabricPool space usage of object stores from capacity-licensed providers has reached the license limit.	Perform the following corrective actions:...Check the percentage of the licensed capacity used by each FabricPool storage tier by using the "storage aggregate object-store show-space" command....Delete Snapshot copies from volumes with the tiering policy "snapshot" or "backup" by using the "volume snapshot delete" command to clear up space....Install a new license on the cluster to increase the licensed capacity.
Giveback of Aggregate Failed	CRITICAL	This event occurs during the migration of an aggregate as part of a storage failover (SFO) giveback, when the destination node cannot reach the object stores.	Perform the following corrective actions:...Verify that your intercluster LIF is online and functional by using the "network interface show" command....Check network connectivity to the object store server by using the "ping" command over the destination node intercluster LIF. ...Verify that the configuration of your object store has not changed and that login and connectivity information is still accurate by using the "aggregate object-store config show" command....Alternatively, you can override the error by specifying false for the "require-partner-waiting" parameter of the giveback command....Contact NetApp technical support for more information or assistance.

HA Interconnect Down	WARNING	<p>The high-availability (HA) interconnect is down. Risk of service outage when failover is not available.</p> <p>Corrective actions depend on the number and type of HA interconnect links supported by the platform, as well as the reason why the interconnect is down.</p> <p>...If the links are down:...Verify that both controllers in the HA pair are operational....For externally connected links, make sure that the interconnect cables are connected properly and that the small form-factor pluggables (SFPs), if applicable, are seated properly on both controllers....For internally connected links, disable and re-enable the links, one after the other, by using the "ic link off" and "ic link on" commands.</p> <p>...If links are disabled, enable the links by using the "ic link on" command.</p> <p>...If a peer is not connected, disable and re-enable the links, one after the other, by using the "ic link off" and "ic link on" commands....Contact NetApp technical support if the issue persists.</p>
----------------------	---------	---

Max Sessions Per User Exceeded	WARNING	<p>You have exceeded the maximum number of sessions allowed per user over a TCP connection. Any request to establish a session will be denied until some sessions are released. ...</p>	<p>Perform the following corrective actions: ...Inspect all the applications that run on the client, and terminate any that are not operating properly....Reboot the client....Check if the issue is caused by a new or existing application:...If the application is new, set a higher threshold for the client by using the "cifs option modify -max-opens -same-file-per-tree" command. In some cases, clients operate as expected, but require a higher threshold. You should have advanced privilege to set a higher threshold for the client. ...If the issue is caused by an existing application, there might be an issue with the client. Contact NetApp technical support for more information or assistance.</p>
--------------------------------	---------	---	---

Max Times Open Per File Exceeded	WARNING	<p>You have exceeded the maximum number of times that you can open the file over a TCP connection. Any request to open this file will be denied until you close some open instances of the file. This typically indicates abnormal application behavior....</p>	<p>Perform the following corrective actions:...Inspect the applications that run on the client using this TCP connection. The client might be operating incorrectly because of the application running on it....Reboot the client....Check if the issue is caused by a new or existing application:...If the application is new, set a higher threshold for the client by using the "cifs option modify -max-opens -same-file-per-tree" command. In some cases, clients operate as expected, but require a higher threshold. You should have advanced privilege to set a higher threshold for the client. ...If the issue is caused by an existing application, there might be an issue with the client. Contact NetApp technical support for more information or assistance.</p>
----------------------------------	---------	---	---

NetBIOS Name Conflict	CRITICAL	The NetBIOS Name Service has received a negative response to a name registration request, from a remote machine. This is typically caused by a conflict in the NetBIOS name or an alias. As a result, clients might not be able to access data or connect to the right data-serving node in the cluster.	Perform any one of the following corrective actions:...If there is a conflict in the NetBIOS name or an alias, perform one of the following:...Delete the duplicate NetBIOS alias by using the "vserver cifs delete -aliases alias -vserver vserver" command....Rename a NetBIOS alias by deleting the duplicate name and adding an alias with a new name by using the "vserver cifs create -aliases alias -vserver vserver" command. ...If there are no aliases configured and there is a conflict in the NetBIOS name, then rename the CIFS server by using the "vserver cifs delete -vserver vserver" and "vserver cifs create -cifs -server netbiosname" commands. NOTE: Deleting a CIFS server can make data inaccessible. ...Remove NetBIOS name or rename the NetBIOS on the remote machine.
NFSv4 Store Pool Exhausted	CRITICAL	A NFSv4 store pool has been exhausted.	If the NFS server is unresponsive for more than 10 minutes after this event, contact NetApp technical support.
No Registered Scan Engine	CRITICAL	The antivirus connector notified ONTAP that it does not have a registered scan engine. This might cause data unavailability if the "scan-mandatory" option is enabled.	Perform the following corrective actions:...Ensure that the scan engine software installed on the antivirus server is compatible with ONTAP....Ensure that scan engine software is running and configured to connect to the antivirus connector over local loopback.

No Vscan Connection	CRITICAL	ONTAP has no Vscan connection to service virus scan requests. This might cause data unavailability if the "scan-mandatory" option is enabled.	Ensure that the scanner pool is properly configured and the antivirus servers are active and connected to ONTAP.
Node Root Volume Space Low	CRITICAL	The system has detected that the root volume is dangerously low on space. The node is not fully operational. Data LIFs might have failed over within the cluster, because of which NFS and CIFS access is limited on the node. Administrative capability is limited to local recovery procedures for the node to clear up space on the root volume.	Perform the following corrective actions:...Clear up space on the root volume by deleting old Snapshot copies, deleting files you no longer need from the /mroot directory, or expanding the root volume capacity....Reboot the controller....Contact NetApp technical support for more information or assistance.
Nonexistent Admin Share	CRITICAL	Vscan issue: a client has attempted to connect to a nonexistent ONTAP_ADMIN\$ share.	Ensure that Vscan is enabled for the mentioned SVM ID. Enabling Vscan on a SVM causes the ONTAP_ADMIN\$ share to be created for the SVM automatically.
NVMe Namespace Out of Space	CRITICAL	An NVMe namespace has been brought offline because of a write failure caused by lack of space.	Add space to the volume, and then bring the NVMe namespace online by using the "vserver nvme namespace modify" command.
NVMe-oF Grace Period Active	WARNING	This event occurs on a daily basis when the NVMe over Fabrics (NVMe-oF) protocol is in use and the grace period of the license is active. The NVMe-oF functionality requires a license after the license grace period expires. NVMe-oF functionality is disabled when the license grace period is over.	Contact your sales representative to obtain an NVMe-oF license, and add it to the cluster, or remove all instances of NVMe-oF configuration from the cluster.

NVMe-oF Grace Period Expired	WARNING	The NVMe over Fabrics (NVMe-oF) license grace period is over and the NVMe-oF functionality is disabled.	Contact your sales representative to obtain an NVMe-oF license, and add it to the cluster.
NVMe-oF Grace Period Start	WARNING	The NVMe over Fabrics (NVMe-oF) configuration was detected during the upgrade to ONTAP 9.5 software. NVMe-oF functionality requires a license after the license grace period expires.	Contact your sales representative to obtain an NVMe-oF license, and add it to the cluster.
Object Store Host Unresolvable	CRITICAL	The object store server host name cannot be resolved to an IP address. The object store client cannot communicate with the object-store server without resolving to an IP address. As a result, data might be inaccessible.	Check the DNS configuration to verify that the host name is configured correctly with an IP address.
Object Store Intercluster LIF Down	CRITICAL	The object-store client cannot find an operational LIF to communicate with the object store server. The node will not allow object store client traffic until the intercluster LIF is operational. As a result, data might be inaccessible.	Perform the following corrective actions:...Check the intercluster LIF status by using the "network interface show -role intercluster" command....Verify that the intercluster LIF is configured correctly and operational....If an intercluster LIF is not configured, add it by using the "network interface create -role intercluster" command.
Object Store Signature Mismatch	CRITICAL	The request signature sent to the object store server does not match the signature calculated by the client. As a result, data might be inaccessible.	Verify that the secret access key is configured correctly. If it is configured correctly, contact NetApp technical support for assistance.

REaddir Timeout	CRITICAL	A REaddir file operation has exceeded the timeout that it is allowed to run in WAFL. This can be because of very large or sparse directories. Corrective action is recommended.	Perform the following corrective actions:...Find information specific to recent directories that have had REaddir file operations expire by using the following 'diag' privilege nodeshell CLI command: wafl readdir notice show....Check if directories are indicated as sparse or not:...If a directory is indicated as sparse, it is recommended that you copy the contents of the directory to a new directory to remove the sparseness of the directory file.If a directory is not indicated as sparse and the directory is large, it is recommended that you reduce the size of the directory file by reducing the number of file entries in the directory.
-----------------	----------	---	---

Relocation of Aggregate Failed	CRITICAL	This event occurs during the relocation of an aggregate, when the destination node cannot reach the object stores.	Perform the following corrective actions:...Verify that your intercluster LIF is online and functional by using the "network interface show" command....Check network connectivity to the object store server by using the "ping" command over the destination node intercluster LIF. ...Verify that the configuration of your object store has not changed and that login and connectivity information is still accurate by using the "aggregate object-store config show" command....Alternatively, you can override the error by using the "override-destination-checks" parameter of the relocation command....Contact NetApp technical support for more information or assistance.
Shadow Copy Failed	CRITICAL	A Volume Shadow Copy Service (VSS), a Microsoft Server backup and restore service operation, has failed.	Check the following using the information provided in the event message:...Is shadow copy configuration enabled?...Are the appropriate licenses installed? ...On which shares is the shadow copy operation performed?...Is the share name correct?...Does the share path exist?...What are the states of the shadow copy set and its shadow copies?

Storage Switch Power Supplies Failed	WARNING	There is a missing power supply in the cluster switch. Redundancy is reduced, risk of outage with any further power failures.	Perform the following corrective actions:...Ensure that the power supply mains, which supplies power to the cluster switch, is turned on....Ensure that the power cord is connected to the power supply....Contact NetApp technical support if the issue persists.
Too Many CIFS Authentication	WARNING	Many authentication negotiations have occurred simultaneously. There are 256 incomplete new session requests from this client.	Investigate why the client has created 256 or more new connection requests. You might have to contact the vendor of the client or of the application to determine why the error occurred.
Unauthorized User Access to Admin Share	WARNING	A client has attempted to connect to the privileged ONTAP_ADMIN\$ share even though their logged-in user is not an allowed user.	Perform the following corrective actions:...Ensure that the mentioned username and IP address is configured in one of the active Vscan scanner pools....Check the scanner pool configuration that is currently active by using the "vserver vscan scanner pool show-active" command.
Virus Detected	WARNING	A Vscan server has reported an error to the storage system. This typically indicates that a virus has been found. However, other errors on the Vscan server can cause this event....Client access to the file is denied. The Vscan server might, depending on its settings and configuration, clean the file, quarantine it, or delete it.	Check the log of the Vscan server reported in the "syslog" event to see if it was able to successfully clean, quarantine, or delete the infected file. If it was not able to do so, a system administrator might have to manually delete the file.
Volume Offline	INFO	This message indicates that a volume is made offline.	Bring the volume back online.

Volume Restricted	INFO	This event indicates that a flexible volume is made restricted.	Bring the volume back online.
Storage VM Stop Succeeded	INFO	This message occurs when a 'vserver stop' operation succeeds.	Use 'vserver start' command to start the data access on a storage VM.
Node Panic	WARNING	This event is issued when a panic occurs	Contact NetApp customer support.

[Back to Top](#)

Anti-Ransomware Log Monitors

Monitor Name	Severity	Description	Corrective Action
Storage VM Anti-ransomware Monitoring Disabled	WARNING	The anti-ransomware monitoring for the storage VM is disabled. Enable anti-ransomware to protect the storage VM.	None
Storage VM Anti-ransomware Monitoring Enabled (Learning Mode)	INFO	The anti-ransomware monitoring for the storage VM is enabled in learning mode.	None
Volume Anti-ransomware Monitoring Enabled	INFO	The anti-ransomware monitoring for the volume is enabled.	None
Volume Anti-ransomware Monitoring Disabled	WARNING	The anti-ransomware monitoring for the volume is disabled. Enable anti-ransomware to protect the volume.	None
Volume Anti-ransomware Monitoring Enabled (Learning Mode)	INFO	The anti-ransomware monitoring for the volume is enabled in learning mode.	None
Volume Anti-ransomware Monitoring Paused (Learning Mode)	WARNING	The anti-ransomware monitoring for the volume is paused in learning mode.	None
Volume Anti-ransomware Monitoring Paused	WARNING	The anti-ransomware monitoring for the volume is paused.	None
Volume Anti-ransomware Monitoring Disabling	WARNING	The anti-ransomware monitoring for the volume is disabling.	None

Ransomware Activity Detected	CRITICAL	<p>To protect the data from the detected ransomware, a Snapshot copy has been taken that can be used to restore original data.</p> <p>Your system generates and transmits an AutoSupport or "call home" message to NetApp technical support and any configured destinations. AutoSupport message improves problem determination and resolution.</p>	Refer to the "FINAL-DOCUMENT-NAME" to take remedial measures for ransomware activity.
------------------------------	----------	---	---

[Back to Top](#)

FSx for NetApp ONTAP Monitors

Monitor Name	Thresholds	Monitor Description	Corrective Action
FSx Volume Capacity is Full	Warning @ > 85 %...Critical @ > 95 %	<p>Storage capacity of a volume is necessary to store application and customer data. The more data stored in the ONTAP volume the less storage availability for future data. If the data storage capacity within a volume reaches the total storage capacity may lead to the customer being unable to store data due to lack of storage capacity. Monitoring the volume used storage capacity ensures data services continuity.</p>	<p>Immediate actions are required to minimize service disruption if critical threshold is breached:</p> <ol style="list-style-type: none"> 1. Consider deleting data that is not needed anymore to free up space

FSx Volume High Latency	Warning @ > 1000 µs...Critical @ > 2000 µs	<p>Volumes are objects that serve the IO traffic often driven by performance sensitive applications including devOps applications, home directories, and databases. High volume latencies means that the applications themselves may suffer and be unable to accomplish their tasks. Monitoring volume latencies is critical to maintain application consistent performance.</p>	<p>Immediate actions are required to minimize service disruption if critical threshold is breached:...1. If the volume has a QoS policy assigned to it, evaluate its limit thresholds in case they are causing the volume workload to get throttled.....Plan to take the following actions soon if warning threshold is breached:...1. If the volume has a QoS policy assigned to it, evaluate its limit thresholds in case they are causing the volume workload to get throttled....2. If the node is also experiencing high utilization, move the volume to another node or reduce the total workload of the node.</p>
FSx Volume Inodes Limit	Warning @ > 85 %...Critical @ > 95 %	<p>Volumes that store files use index nodes (inode) to store file metadata. When a volume exhausts its inode allocation no more files can be added to it. A warning alert indicates that planned action should be taken to increase the number of available inodes. A critical alert indicates that file limit exhaustion is imminent and emergency measures should be taken to free up inodes to ensure service continuity</p>	<p>Immediate actions are required to minimize service disruption if critical threshold is breached:...1. Consider increasing the inodes value for the volume. If the inodes value is already at the max, then consider splitting the volume into two or more volumes because the file system has grown beyond the maximum size.....Plan to take the following actions soon if warning threshold is breached:...1. Consider increasing the inodes value for the volume. If the inodes value is already at the max, then consider splitting the volume into two or more volumes because the file system has grown beyond the maximum size</p>

FSx Volume Qtree Quota Overcommit	Warning @ > 95 %...Critical @ > 100 %	<p>Volume Qtree Quota Overcommit specifies the percentage at which a volume is considered to be overcommitted by the qtree quotas. The set threshold for the qtree quota is reached for the volume. Monitoring the volume qtree quota overcommit ensures that the user receives uninterrupted data service.</p>	<p>If critical threshold is breached, then immediate actions should be taken to minimize service disruption:</p> <ol style="list-style-type: none"> 1. Delete unwanted data...When warning threshold is breached, then consider increasing the space of the volume.
FSx Snapshot Reserve Space is Full	Warning @ > 90 %...Critical @ > 95 %	<p>Storage capacity of a volume is necessary to store application and customer data. A portion of that space, called snapshot reserved space, is used to store snapshots which allow data to be protected locally. The more new and updated data stored in the ONTAP volume the more snapshot capacity is used and less snapshot storage capacity will be available for future new or updated data. If the snapshot data capacity within a volume reaches the total snapshot reserve space it may lead to the customer being unable to store new snapshot data and reduction in the level of protection for the data in the volume. Monitoring the volume used snapshot capacity ensures data services continuity.</p>	<p>Immediate actions are required to minimize service disruption if critical threshold is breached:...1. Consider configuring snapshots to use data space in the volume when the snapshot reserve is full...2. Consider deleting some older snapshots that may not be needed anymore to free up space.....Plan to take the following actions soon if warning threshold is breached:...1. Consider increasing the snapshot reserve space within the volume to accommodate the growth...2. Consider configuring snapshots to use data space in the volume when the snapshot reserve is full</p>

FSx Volume Cache Miss Ratio	Warning @ > 95 %...Critical @ > 100 %	Volume Cache Miss Ratio is the percentage of read requests from the client applications that are returned from the disk instead of being returned from the cache. This means that the volume has reached the set threshold.	If critical threshold is breached, then immediate actions should be taken to minimize service disruption: 1. Move some workloads off of the node of the volume to reduce the IO load 2. Lower the demand of lower priority workloads on the same node via QoS limits...Consider immediate actions when warning threshold is breached: 1. Move some workloads off of the node of the volume to reduce the IO load 2. Lower the demand of lower priority workloads on the same node via QoS limits 3. Change workload characteristics (block size, application caching etc)
-----------------------------	---------------------------------------	---	--

[Back to Top](#)

K8s Monitors

Monitor Name	Severity	Monitor Description
POD Created	Informational	This alert occurs when a POD is created.
POD Deleted	Informational	This alert occurs when a POD is deleted.
Daemonset Created	Informational	This alert occurs when a Daemonset is created.
Daemonset Deleted	Informational	This alert occurs when a Daemonset is deleted.
Replicaset Created	Informational	This alert occurs when a Replicaset is created.
Replicaset Deleted	Informational	This alert occurs when a Replicaset is deleted.
Deployment Created	Informational	This alert occurs when a Deployment is created.

POD Failed	WARNING	This alert occurs when a POD is failed.
POD Attach Failed	WARNING	This alert occurs when a volume attachment with POD is failed.
Persistent Volume Claim Failed Binding	WARNING	This alert occurs when a binding is failed on a PVC.
POD Failed Mount	WARNING	This alert occurs when a mount is failed on a POD.

[Back to Top](#)

Change Log Monitors

Monitor Name	Severity	Monitor Description
Internal Volume Discovered	Informational	This message occurs when an Internal Volume is discovered.
Internal Volume Modified	Informational	This message occurs when an Internal Volume is modified.
Storage Node Discovered	Informational	This message occurs when an Storage Node is discovered.
Storage Node Removed	Informational	This message occurs when an Storage Node is removed.
Storage Pool Discovered	Informational	This message occurs when an Storage Pool is discovered.
Storage Virtual Machine Discovered	Informational	This message occurs when an Storage Virtual Machine is discovered.
Storage Virtual Machine Modified	Informational	This message occurs when an Storage Virtual Machine is modified.

[Back to Top](#)

Data Collection Monitors

Monitor Name	Description	Corrective Action

Acquisition Unit Shutdown	Cloud Insights Acquisition Units periodically restart as part of upgrades to introduce new features. This happens once a month or less in a typical environment. A Warning Alert that an Acquisition Unit has shutdown should be followed soon after by a Resolution noting that the newly-restarted Acquisition Unit has completed a registration with Cloud Insights. Typically this shutdown-to-registration cycle takes 5 to 15 minutes.	If the alert occurs frequently or lasts longer than 15 minutes, check on the operation of the system hosting the Acquisition Unit, the network, and any proxy connecting the AU to the Internet.
Collector Failed	The poll of a data collector encountered an unexpected failure situation.	Visit the data collector page in Cloud Insights to learn more about the situation.
Collector Warning	This Alert typically can arise because of an erroneous configuration of the data collector or of the target system. Revisit the configurations to prevent future Alerts. It can also be due to a retrieval of less-than-complete data where the data collector gathered all the data that it could. This can happen when situations change during data collection (e.g., a virtual machine present at the beginning of data collection is deleted during data collection and before its data is captured).	Check the configuration of the data collector or target system. Note that the monitor for Collector Warning can send more alerts than other monitor types, so it is recommended to set no alert recipients unless you are troubleshooting.

[Back to Top](#)

Security Monitors

Monitor Name	Threshold	Monitor Description	Corrective Action
AutoSupport HTTPS transport disabled	Warning @ < 1	AutoSupport supports HTTPS, HTTP, and SMTP for transport protocols. Because of the sensitive nature of AutoSupport messages, NetApp strongly recommends using HTTPS as the default transport protocol for sending AutoSupport messages to NetApp support.	To set HTTPS as the transport protocol for AutoSupport messages, run the following ONTAP command:...system node autosupport modify -transport https

Cluster Insecure ciphers for SSH	Warning @ < 1	Indicates that SSH is using insecure ciphers, for example ciphers beginning with *cbc.	To remove the CBC ciphers, run the following ONTAP command:...security ssh remove -vserver <admin vserver> -ciphers aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc
Cluster Login Banner Disabled	Warning @ < 1	Indicates that the Login banner is disabled for users accessing the ONTAP system. Displaying a login banner is helpful for establishing expectations for access and use of the system.	To configure the login banner for a cluster, run the following ONTAP command:...security login banner modify -vserver <admin svm> -message "Access restricted to authorized users"
Cluster Peer Communication Not Encrypted	Warning @ < 1	When replicating data for disaster recovery, caching, or backup, you must protect that data during transport over the wire from one ONTAP cluster to another. Encryption must be configured on both the source and destination clusters.	To enable encryption on cluster peer relationships that were created prior to ONTAP 9.6, the source and destination cluster must be upgraded to 9.6. Then use the "cluster peer modify" command to change both the source and destination cluster peers to use Cluster Peering Encryption....See the NetApp Security Hardening Guide for ONTAP 9 for details.
Default Local Admin User Enabled	Warning @ > 0	NetApp recommends locking (disabling) any unneeded Default Admin User (built-in) accounts with the lock command. They are primarily default accounts for which passwords were never updated or changed.	To lock the built-in "admin" account, run the following ONTAP command:...security login lock -username admin
FIPS Mode Disabled	Warning @ < 1	When FIPS 140-2 compliance is enabled, TLSv1 and SSLv3 are disabled, and only TLSv1.1 and TLSv1.2 remain enabled. ONTAP prevents you from enabling TLSv1 and SSLv3 when FIPS 140-2 compliance is enabled.	To enable FIPS 140-2 compliance on a cluster, run the following ONTAP command in advanced privilege mode:...security config modify -interface SSL -is-fips-enabled true

Log Forwarding Not Encrypted	Warning @ < 1	Offloading of syslog information is necessary for limiting the scope or footprint of a breach to a single system or solution. Therefore, NetApp recommends securely offloading syslog information to a secure storage or retention location.	Once a log forwarding destination is created, its protocol cannot be changed. To change to an encrypted protocol, delete and recreate the log forwarding destination using the following ONTAP command: ...cluster log-forwarding create -destination <destination ip> -protocol tcp-encrypted
MD5 Hashed password	Warning @ > 0	NetApp strongly recommends to use the more secure SHA-512 hash function for ONTAP user account passwords. Accounts using the less secure MD5 hash function should migrate to the SHA-512 hash function.	NetApp strongly recommends user accounts migrate to the more secure SHA-512 solution by having users change their passwords....to lock accounts with passwords that use the MD5 hash function, run the following ONTAP command: ...security login lock -vserver * -username * -hash-function md5
No NTP servers are configured	Warning @ < 1	Indicates that the cluster has no configured NTP servers. For redundancy and optimum service, NetApp recommends that you associate at least three NTP servers with the cluster.	To associate an NTP server with the cluster, run the following ONTAP command: cluster time-service ntp server create -server <ntp server host name or ip address>
NTP server count is low	Warning @ < 3	Indicates that the cluster has less than 3 configured NTP servers. For redundancy and optimum service, NetApp recommends that you associate at least three NTP servers with the cluster.	To associate an NTP server with the cluster, run the following ONTAP command: ...cluster time-service ntp server create -server <ntp server host name or ip address>

Remote Shell Enabled	Warning @ > 0	Remote Shell is not a secure method for establishing command-line access to the ONTAP solution. Remote Shell should be disabled for secure remote access.	NetApp recommends Secure Shell (SSH) for secure remote access....To disable Remote shell on a cluster, run the following ONTAP command in advanced privilege mode:...security protocol modify -application rsh- enabled false
Storage VM Audit Log Disabled	Warning @ < 1	Indicates that Audit logging is disabled for SVM.	To configure the Audit log for a vserver, run the following ONTAP command:...vserver audit enable -vserver <svm>
Storage VM Insecure ciphers for SSH	Warning @ < 1	Indicates that SSH is using insecure ciphers, for example ciphers beginning with *cbc.	To remove the CBC ciphers, run the following ONTAP command:...security ssh remove -vserver <vserver> -ciphers aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc
Storage VM Login banner disabled	Warning @ < 1	Indicates that the Login banner is disabled for users accessing SVMs on the system. Displaying a login banner is helpful for establishing expectations for access and use of the system.	To configure the login banner for a cluster, run the following ONTAP command:...security login banner modify -vserver <svm> -message "Access restricted to authorized users"
Telnet Protocol Enabled	Warning @ > 0	Telnet is not a secure method for establishing command-line access to the ONTAP solution. Telnet should be disabled for secure remote access.	NetApp recommends Secure Shell (SSH) for secure remote access. To disable Telnet on a cluster, run the following ONTAP command in advanced privilege mode:...security protocol modify -application telnet -enabled false

[Back to Top](#)

Data Protection Monitors

Monitor Name	Thresholds	Monitor Description	Corrective Action
--------------	------------	---------------------	-------------------

Insufficient Space for Lun Snapshot Copy	(Filter contains_luns = Yes) Warning @ > 95 %...Critical @ > 100 %	<p>Storage capacity of a volume is necessary to store application and customer data. A portion of that space, called snapshot reserved space, is used to store snapshots which allow data to be protected locally. The more new and updated data stored in the ONTAP volume the more snapshot capacity is used and less snapshot storage capacity will be available for future new or updated data. If the snapshot data capacity within a volume reaches the total snapshot reserve space it may lead to the customer being unable to store new snapshot data and reduction in the level of protection for the data in the LUNs in the volume. Monitoring the volume used snapshot capacity ensures data services continuity.</p>	<p>Immediate Actions</p> <p>If critical threshold is breached, consider immediate actions to minimize service disruption:</p> <ol style="list-style-type: none"> 1. Configure snapshots to use data space in the volume when the snapshot reserve is full. 2. Delete some older unwanted snapshots to free up space. <p>Actions To Do Soon</p> <p>If warning threshold is breached, plan to take the following immediate actions:</p> <ol style="list-style-type: none"> 1. Increase the snapshot reserve space within the volume to accommodate the growth. 2. Configure snapshots to use data space in the volume when the snapshot reserve is full.
SnapMirror Relationship Lag	Warning @ > 150%...Critical @ > 300%	<p>SnapMirror relationship lag is the difference between the snapshot timestamp and the time on the destination system. The lag_time_percent is the ratio of lag time to the SnapMirror Policy's schedule interval. If the lag time equals the schedule interval, the lag_time_percent will be 100%. If the SnapMirror policy does not have a schedule, lag_time_percent will not be calculated.</p>	<p>Monitor SnapMirror status using the "snapmirror show" command. Check the SnapMirror transfer history using the "snapmirror show-history" command</p>

[Back to Top](#)

Cloud Volume (CVO) Monitors

Monitor Name	CI Severity	Monitor Description	Corrective Action
--------------	-------------	---------------------	-------------------

CVO Disk Out of Service	INFO	This event occurs when a disk is removed from service because it has been marked failed, is being sanitized, or has entered the Maintenance Center.	None
CVO Giveback of Storage Pool Failed	CRITICAL	<p>This event occurs during the migration of an aggregate as part of a storage failover (SFO) giveback, when the destination node cannot reach the object stores.</p>	<p>Perform the following corrective actions:</p> <p>Verify that your intercluster LIF is online and functional by using the "network interface show" command.</p> <p>Check network connectivity to the object store server by using the "ping" command over the destination node intercluster LIF.</p> <p>Verify that the configuration of your object store has not changed and that login and connectivity information is still accurate by using the "aggregate object-store config show" command.</p> <p>Alternatively, you can override the error by specifying false for the "require-partner-waiting" parameter of the giveback command.</p> <p>Contact NetApp technical support for more information or assistance.</p>

CVO HA Interconnect Down	WARNING	<p>The high-availability (HA) interconnect is down. Risk of service outage when failover is not available.</p> <p>Corrective actions depend on the number and type of HA interconnect links supported by the platform, as well as the reason why the interconnect is down.</p> <p>If the links are down:</p> <p>Verify that both controllers in the HA pair are operational.</p> <p>For externally connected links, make sure that the interconnect cables are connected properly and that the small form-factor pluggables (SFPs), if applicable, are seated properly on both controllers.</p> <p>For internally connected links, disable and re-enable the links, one after the other, by using the "ic link off" and "ic link on" commands.</p> <p>If links are disabled, enable the links by using the "ic link on" command.</p> <p>If a peer is not connected, disable and re-enable the links, one after the other, by using the "ic link off" and "ic link on" commands.</p> <p>Contact NetApp technical support if the issue persists.</p>
--------------------------	---------	--

CVO Max Sessions Per User Exceeded	WARNING	<p>You have exceeded the maximum number of sessions allowed per user over a TCP connection. Any request to establish a session will be denied until some sessions are released.</p>	<p>Perform the following corrective actions:</p> <ul style="list-style-type: none"> Inspect all the applications that run on the client, and terminate any that are not operating properly. Reboot the client. Check if the issue is caused by a new or existing application: <ul style="list-style-type: none"> If the application is new, set a higher threshold for the client by using the "cifs option modify -max-opens -same-file-per-tree" command. In some cases, clients operate as expected, but require a higher threshold. You should have advanced privilege to set a higher threshold for the client. If the issue is caused by an existing application, there might be an issue with the client. Contact NetApp technical support for more information or assistance.
------------------------------------	---------	---	--

CVO NetBIOS Name Conflict	CRITICAL	<p>The NetBIOS Name Service has received a negative response to a name registration request, from a remote machine. This is typically caused by a conflict in the NetBIOS name or an alias. As a result, clients might not be able to access data or connect to the right data-serving node in the cluster.</p>	<p>Perform any one of the following corrective actions:</p> <p>If there is a conflict in the NetBIOS name or an alias, perform one of the following:</p> <ul style="list-style-type: none"> Delete the duplicate NetBIOS alias by using the "vserver cifs delete -aliases alias -vserver vserver" command. Rename a NetBIOS alias by deleting the duplicate name and adding an alias with a new name by using the "vserver cifs create -aliases alias -vserver vserver" command. If there are no aliases configured and there is a conflict in the NetBIOS name, then rename the CIFS server by using the "vserver cifs delete -vserver vserver" and "vserver cifs create -cifs -server netbiosname" commands. NOTE: Deleting a CIFS server can make data inaccessible. Remove NetBIOS name or rename the NetBIOS on the remote machine.
CVO NFSv4 Store Pool Exhausted	CRITICAL	A NFSv4 store pool has been exhausted.	If the NFS server is unresponsive for more than 10 minutes after this event, contact NetApp technical support.
CVO Node Panic	WARNING	This event is issued when a panic occurs	Contact NetApp customer support.

CVO Node Root Volume Space Low	CRITICAL	<p>The system has detected that the root volume is dangerously low on space. The node is not fully operational. Data LIFs might have failed over within the cluster, because of which NFS and CIFS access is limited on the node.</p> <p>Administrative capability is limited to local recovery procedures for the node to clear up space on the root volume.</p>	<p>Perform the following corrective actions:</p> <p>Clear up space on the root volume by deleting old Snapshot copies, deleting files you no longer need from the /mroot directory, or expanding the root volume capacity.</p> <p>Reboot the controller.</p> <p>Contact NetApp technical support for more information or assistance.</p>
CVO Nonexistent Admin Share	CRITICAL	Vscan issue: a client has attempted to connect to a nonexistent ONTAP_ADMIN\$ share.	Ensure that Vscan is enabled for the mentioned SVM ID. Enabling Vscan on a SVM causes the ONTAP_ADMIN\$ share to be created for the SVM automatically.
CVO Object Store Host Unresolvable	CRITICAL	The object store server host name cannot be resolved to an IP address. The object store client cannot communicate with the object-store server without resolving to an IP address. As a result, data might be inaccessible.	Check the DNS configuration to verify that the host name is configured correctly with an IP address.
CVO Object Store Intercluster LIF Down	CRITICAL	The object-store client cannot find an operational LIF to communicate with the object store server. The node will not allow object store client traffic until the intercluster LIF is operational. As a result, data might be inaccessible.	<p>Perform the following corrective actions:</p> <p>Check the intercluster LIF status by using the "network interface show -role intercluster" command.</p> <p>Verify that the intercluster LIF is configured correctly and operational.</p> <p>If an intercluster LIF is not configured, add it by using the "network interface create -role intercluster" command.</p>

CVO Object Store Signature Mismatch	CRITICAL	The request signature sent to the object store server does not match the signature calculated by the client. As a result, data might be inaccessible.	Verify that the secret access key is configured correctly. If it is configured correctly, contact NetApp technical support for assistance.
CVO QoS Monitor Memory Maxed Out	CRITICAL	The QoS subsystem's dynamic memory has reached its limit for the current platform hardware. Some QoS features might operate in a limited capacity.	Delete some active workloads or streams to free up memory. Use the "statistics show -object workload -counter ops" command to determine which workloads are active. Active workloads show non-zero ops. Then use the "workload delete <workload_name>" command multiple times to remove specific workloads. Alternatively, use the "stream delete -workload <workload name> *" command to delete the associated streams from the active workload.

CVO REaddir Timeout	CRITICAL	<p>A REaddir file operation has exceeded the timeout that it is allowed to run in WAFL. This can be because of very large or sparse directories. Corrective action is recommended.</p>	<p>Perform the following corrective actions:</p> <p>Find information specific to recent directories that have had REaddir file operations expire by using the following 'diag' privilege nodeshell CLI command: wafl readdir notice show.</p> <p>Check if directories are indicated as sparse or not:</p> <p>If a directory is indicated as sparse, it is recommended that you copy the contents of the directory to a new directory to remove the sparseness of the directory file.</p> <p>If a directory is not indicated as sparse and the directory is large, it is recommended that you reduce the size of the directory file by reducing the number of file entries in the directory.</p>
---------------------	----------	--	---

CVO Relocation of Storage Pool Failed	CRITICAL	<p>This event occurs during the relocation of an aggregate, when the destination node cannot reach the object stores.</p>	<p>Perform the following corrective actions:</p> <p>Verify that your intercluster LIF is online and functional by using the "network interface show" command.</p> <p>Check network connectivity to the object store server by using the "ping" command over the destination node intercluster LIF.</p> <p>Verify that the configuration of your object store has not changed and that login and connectivity information is still accurate by using the "aggregate object-store config show" command.</p> <p>Alternatively, you can override the error by using the "override-destination-checks" parameter of the relocation command.</p> <p>Contact NetApp technical support for more information or assistance.</p>
---------------------------------------	----------	---	--

CVO Shadow Copy Failed	CRITICAL	A Volume Shadow Copy Service (VSS), a Microsoft Server backup and restore service operation, has failed.	<p>Check the following using the information provided in the event message:</p> <p>Is shadow copy configuration enabled?</p> <p>Are the appropriate licenses installed?</p> <p>On which shares is the shadow copy operation performed?</p> <p>Is the share name correct?</p> <p>Does the share path exist?</p> <p>What are the states of the shadow copy set and its shadow copies?</p>
CVO Storage VM Stop Succeeded	INFO	This message occurs when a 'vserver stop' operation succeeds.	Use 'vserver start' command to start the data access on a storage VM.
CVO Too Many CIFS Authentication	WARNING	Many authentication negotiations have occurred simultaneously. There are 256 incomplete new session requests from this client.	Investigate why the client has created 256 or more new connection requests. You might have to contact the vendor of the client or of the application to determine why the error occurred.
CVO Unassigned Disks	INFO	System has unassigned disks - capacity is being wasted and your system may have some misconfiguration or partial configuration change applied.	<p>Perform the following corrective actions:</p> <p>Determine which disks are unassigned by using the "disk show -n" command.</p> <p>Assign the disks to a system by using the "disk assign" command.</p>

CVO Unauthorized User Access to Admin Share	WARNING	<p>A client has attempted to connect to the privileged ONTAP_ADMIN\$ share even though their logged in user is not an allowed user.</p>	<p>Perform the following corrective actions:</p> <p>Ensure that the mentioned username and IP address is configured in one of the active Vscan scanner pools.</p> <p>Check the scanner pool configuration that is currently active by using the "vserver vscan scanner pool show-active" command.</p>
CVO Virus Detected	WARNING	<p>A Vscan server has reported an error to the storage system. This typically indicates that a virus has been found. However, other errors on the Vscan server can cause this event.</p> <p>Client access to the file is denied. The Vscan server might, depending on its settings and configuration, clean the file, quarantine it, or delete it.</p>	<p>Check the log of the Vscan server reported in the "syslog" event to see if it was able to successfully clean, quarantine, or delete the infected file. If it was not able to do so, a system administrator might have to manually delete the file.</p>
CVO Volume Offline	INFO	This message indicates that a volume is made offline.	Bring the volume back online.
CVO Volume Restricted	INFO	This event indicates that a flexible volume is made restricted.	Bring the volume back online.

[Back to Top](#)

SnapMirror for Business Continuity (SMBC) Mediator Log Monitors

Monitor Name	Severity	Monitor Description	Corrective Action
ONTAP Mediator Added	INFO	This message occurs when ONTAP Mediator is added successfully on a cluster.	None

ONTAP Mediator Not Accessible	CRITICAL	This message occurs when either the ONTAP Mediator is repurposed or the Mediator package is no longer installed on the Mediator server. As a result, SnapMirror failover is not possible.	Remove the configuration of the current ONTAP Mediator by using the "snapmirror mediator remove" command. Reconfigure access to the ONTAP Mediator by using the "snapmirror mediator add" command.
ONTAP Mediator Removed	INFO	This message occurs when ONTAP Mediator is removed successfully from a cluster.	None
ONTAP Mediator Unreachable	WARNING	This message occurs when the ONTAP Mediator is unreachable on a cluster. As a result, SnapMirror failover is not possible.	Check the network connectivity to the ONTAP Mediator by using the "network ping" and "network traceroute" commands. If the issue persists, remove the configuration of the current ONTAP Mediator by using the "snapmirror mediator remove" command. Reconfigure access to the ONTAP Mediator by using the "snapmirror mediator add" command.
SMBC CA Certificate Expired	CRITICAL	This message occurs when the ONTAP Mediator certificate authority (CA) certificate has expired. As a result, all further communication to the ONTAP Mediator will not be possible.	Remove the configuration of the current ONTAP Mediator by using the "snapmirror mediator remove" command. Update a new CA certificate on the ONTAP Mediator server. Reconfigure access to the ONTAP Mediator by using the "snapmirror mediator add" command.

SMBC CA Certificate Expiring	WARNING	This message occurs when the ONTAP Mediator certificate authority (CA) certificate is due to expire within the next 30 days.	Before this certificate expires, remove the configuration of the current ONTAP Mediator by using the "snapmirror mediator remove" command. Update a new CA certificate on the ONTAP Mediator server. Reconfigure access to the ONTAP Mediator by using the "snapmirror mediator add" command.
SMBC Client Certificate Expired	CRITICAL	This message occurs when the ONTAP Mediator client certificate has expired. As a result, all further communication to the ONTAP Mediator will not be possible.	Remove the configuration of the current ONTAP Mediator by using the "snapmirror mediator remove" command. Reconfigure access to the ONTAP Mediator by using the "snapmirror mediator add" command.
SMBC Client Certificate Expiring	WARNING	This message occurs when the ONTAP Mediator client certificate is due to expire within the next 30 days.	Before this certificate expires, remove the configuration of the current ONTAP Mediator by using the "snapmirror mediator remove" command. Reconfigure access to the ONTAP Mediator by using the "snapmirror mediator add" command.
SMBC Relationship Out of Sync Note: UM doesn't have this one	CRITICAL	This message occurs when a SnapMirror for Business Continuity (SMBC) relationship changes status from "in-sync" to "out-of-sync". Due to this RPO=0 data protection will be disrupted.	Check the network connection between the source and destination volumes. Monitor the SMBC relationship status by using the "snapmirror show" command on the destination, and by using the "snapmirror list-destinations" command on the source. Auto-resync will attempt to bring the relationship back to "in-sync" status. If the resync fails, verify that all the nodes in the cluster are in quorum and are healthy.

SMBC Server Certificate Expired	CRITICAL	This message occurs when the ONTAP Mediator server certificate has expired. As a result, all further communication to the ONTAP Mediator will not be possible.	Remove the configuration of the current ONTAP Mediator by using the "snapmirror mediator remove" command. Update a new server certificate on the ONTAP Mediator server. Reconfigure access to the ONTAP Mediator by using the "snapmirror mediator add" command.
SMBC Server Certificate Expiring	WARNING	This message occurs when the ONTAP Mediator server certificate is due to expire within the next 30 days.	Before this certificate expires, remove the configuration of the current ONTAP Mediator by using the "snapmirror mediator remove" command. Update a new server certificate on the ONTAP Mediator server. Reconfigure access to the ONTAP Mediator by using the "snapmirror mediator add" command.

[Back to Top](#)

Additional Power, Heartbeat, and Miscellaneous System Monitors

Monitor Name	Severity	Monitor Description	Corrective Action
Disk Shelf Power Supply Discovered	INFORMATIONAL	This message occurs when a power supply unit is added to the disk shelf.	NONE
Disk Shelves Power Supply Removed	INFORMATIONAL	This message occurs when a power supply unit is removed from the disk shelf.	NONE
MetroCluster Automatic Unplanned Switchover Disabled	CRITICAL	This message occurs when automatic unplanned switchover capability is disabled.	Run the "metrocluster modify -node-name <nodename> -automatic -switchover-onfailure true" command for each node in the cluster to enable automatic switchover.

Monitor Name	Severity	Monitor Description	Corrective Action
MetroCluster Storage Bridge Unreachable	CRITICAL	The storage bridge is not reachable over the management network	<p>1) If the bridge is monitored by SNMP, verify that the node management LIF is up by using the "network interface show" command. Verify that the bridge is alive by using the "network ping" command.</p> <p>2) If the bridge is monitored in-band, check the fabric cabling to the bridge, and then verify that the bridge is powered up.</p>
MetroCluster Bridge Temperature Abnormal - Below Critical	CRITICAL	The sensor on the Fibre Channel bridge is reporting a temperature that is below the critical threshold.	<p>1) Check the operational status of the fans on the storage bridge.</p> <p>2) Verify that the bridge is operating under recommended temperature conditions.</p>
MetroCluster Bridge Temperature Abnormal - Above Critical	CRITICAL	The sensor on the Fibre Channel bridge is reporting a temperature that is above the critical threshold.	<p>1) Check the operational status of the chassis temperature sensor on the storage bridge using the command "storage bridge show -cooling".</p> <p>2) Verify that the storage bridge is operating under recommended temperature conditions.</p>
MetroCluster Aggregate Left Behind	WARNING	The aggregate was left behind during switchback.	<p>1) Check the aggregate state by using the command "aggr show".</p> <p>2) If the aggregate is online, return it to its original owner by using the command "metrocluster switchback".</p>

Monitor Name	Severity	Monitor Description	Corrective Action
All Links Between Metrocluster Partners Down	CRITICAL	RDMA interconnect adapters and intercluster LIFs have broken connections to the peered cluster or the peered cluster is down.	<p>1) Ensure that the intercluster LIFs are up and running. Repair the intercluster LIFs if they are down.</p> <p>2) Verify that the peered cluster is up and running by using the "cluster peer ping" command. See the MetroCluster Disaster Recovery Guide if the peered cluster is down.</p> <p>3) For fabric MetroCluster, verify that the back-end fabric ISLs are up and running. Repair the back-end fabric ISLs if they are down.</p> <p>4) For non-fabric MetroCluster configurations, verify that the cabling is correct between the RDMA interconnect adapters. Reconfigure the cabling if the links are down.</p>
MetroCluster Partners Not Reachable Over Peering Network	CRITICAL	The connectivity to the peer cluster is broken.	<p>1) Ensure that the port is connected to the correct network/switch.</p> <p>2) Ensure that the intercluster LIF is connected with the peered cluster.</p> <p>3) Ensure that the peered cluster is up and running by using the command "cluster peer ping". Refer to the MetroCluster Disaster Recovery Guide if the peered cluster is down.</p>
MetroCluster Inter Switch All Links Down	CRITICAL	All Inter-Switch Links (ISLs) on the storage switch are down.	<p>1) Repair the back-end fabric ISLs on the storage switch.</p> <p>2) Ensure that the partner switch is up and its ISLs are operational.</p> <p>3) Ensure that intermediate equipment, such as xWDM devices, are operational.</p>

Monitor Name	Severity	Monitor Description	Corrective Action
MetroCluster Node To Storage Stack SAS Link Down	WARNING	The SAS adapter or its attached cable might be at fault.	<ol style="list-style-type: none"> 1. Verify that the SAS adapter is online and running. 2. Verify that the physical cable connection is secure and operating, and replace the cable if necessary. 3. If the SAS adapter is connected to disk shelves, ensure IOMs and disks are properly seated.
MetroClusterFC Initiator Links Down	CRITICAL	The FC initiator adapter is at fault.	<ol style="list-style-type: none"> 1. Ensure that the FC initiator link has not been tampered with. 2. Verify the operational status of the FC initiator adapter by using the command "system node run -node local -command storage show adapter".
FC-VI Interconnect Link Down	CRITICAL	The physical link on the FC-VI port is offline.	<ol style="list-style-type: none"> 1. Ensure that the FC-VI link has not been tampered with. 2. Verify that the physical status of the FC-VI adapter is "Up" by using the command "metrocluster interconnect adapter show". 3. If the configuration includes fabric switches, ensure that they are properly cabled and configured.
MetroCluster Spare Disks Left Behind	WARNING	The spare disk was left behind during switchback.	If the disk is not failed, return it to its original owner by using the command "metrocluster switchback".
MetroCluster Storage Bridge Port Down	CRITICAL	The port on the storage bridge is offline.	<ol style="list-style-type: none"> 1) Check the operational status of the ports on the storage bridge by using the command "storage bridge show -ports". 2) Verify logical and physical connectivity to the port.

Monitor Name	Severity	Monitor Description	Corrective Action
MetroCluster Storage Switch Fans Failed	CRITICAL	The fan on the storage switch failed.	<p>1) Ensure that the fans in the switch are operating correctly by using the command "storage switch show -cooling".</p> <p>2) Ensure that the fan FRUs are properly inserted and operational.</p>
MetroCluster Storage Switch Unreachable	CRITICAL	The storage switch is not reachable over the management network.	<p>1) Ensure that the node management LIF is up by using the command "network interface show".</p> <p>2) Ensure that the switch is alive by using the command "network ping".</p> <p>3) Ensure that the switch is reachable over SNMP by checking its SNMP settings after logging into the switch.</p>
MetroCluster Switch Power Supplies Failed	CRITICAL	A power supply unit on the storage switch is not operational.	<p>1) Check the error details by using the command "storage switch show -error -switch-name <switch name>".</p> <p>2) Identify the faulty power supply unit by using the command "storage switch show -power -switch -name <switch name>".</p> <p>3) Ensure that the power supply units are properly inserted into the chassis of the storage switch and fully operational.</p>
MetroCluster Switch Temperature Sensors Failed	CRITICAL	The sensor on the Fibre Channel switch failed.	<p>1) Check the operational status of the temperature sensors on the storage switch by using the command "storage switch show -cooling".</p> <p>2) Verify that the switch is operating under recommended temperature conditions.</p>

Monitor Name	Severity	Monitor Description	Corrective Action
MetroCluster Switch Temperature Abnormal	CRITICAL	The temperature sensor on the Fibre Channel switch reported abnormal temperature.	<p>1) Check the operational status of the temperature sensors on the storage switch by using the command "storage switch show -cooling".</p> <p>2) Verify that the switch is operating under recommended temperature conditions.</p>
Service Processor Heartbeat Missed	INFORMATIONAL	This message occurs when ONTAP does not receive an expected "heartbeat" signal from the Service Processor (SP). Along with this message, log files from SP will be sent out for debugging. ONTAP will reset the SP to attempt to restore communication. The SP will be unavailable for up to two minutes while it reboots.	Contact NetApp technical support.

Monitor Name	Severity	Monitor Description	Corrective Action
Service Processor Heartbeat Stopped	WARNING	<p>This message occurs when ONTAP is no longer receiving heartbeats from the Service Processor (SP). Depending on the hardware design, the system may continue to serve data or may determine to shut down to prevent data loss or hardware damage. The system continues to serve data, but because the SP might not be working, the system cannot send notifications of down appliances, boot errors, or Open Firmware (OFW) Power-On Self-Test (POST) errors. If your system is configured to do so, it generates and transmits an AutoSupport (or 'call home') message to NetApp technical support and to the configured destinations. Successful delivery of an AutoSupport message significantly improves problem determination and resolution.</p>	<p>If the system has shut down, attempt a hard power cycle: Pull the controller out from the chassis, push it back in then power on the system. Contact NetApp technical support if the problem persists after the power cycle, or for any other condition that may warrant attention.</p>

[Back to Top](#)

More Information

- [Viewing and Dismissing Alerts](#)

Cloud Insights API

The Cloud Insights API enables NetApp customers and independent software vendors (ISVs) to integrate Cloud Insights with other applications, such as CMDB's or other ticketing systems.

Note that Cloud Insights APIs are available based on your current Edition:

API Type	Basic	Standard	Premium
Acquisition Unit	✓	✓	✓
Data Collection	✓	✓	✓
Alerts		✓	✓
Assets		✓	✓
Data Ingestion		✓	✓
Log Ingestion		✓	✓

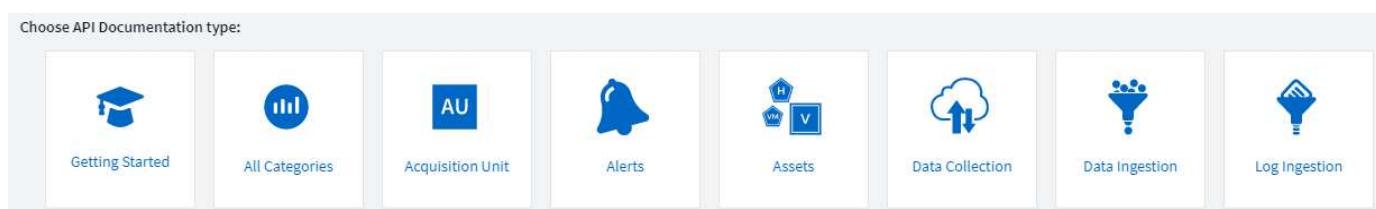
Additionally, your Cloud Insights [feature set role](#) will determine which APIs you can access. User and Guest roles have fewer privileges than Administrator role. For example, if you have Administrator role in Monitor and Optimize, but User role in Reporting, you can manage all API types except Data Warehouse.

Requirements for API Access

- An API Access Token model is used to grant access.
- API Token management is performed by Cloud Insights users with the Administrator role.

API Documentation (Swagger)

The latest API information is found by logging in to Cloud Insights and navigating to **Admin > API Acccess**. Click the [API Documentation](#) link.



The API Documentation is Swagger-based, which provides a brief description and usage information for the API, and allows you to try it out in your environment. Depending on your user role and/or Cloud Insights edition, the API types available to you may vary.

ASSETS.annotations

▼

POST

/assets/annotations Create annotation definition



Parameters

Try it out

No parameters

Request body

application/json

Request body should include required name, type, optional description and enumValues (if enum type). Enums should contain name and label. Example:

```
{  
    "name": "StorageLocation",  
    "type": "FIXED_ENUM",  
    "description": "Storage Location",  
    "enumValues": [  
        {  
            "name": "PT_LISBON",  
            "label": "Lisbon (Portugal)"  
        },  
        {  
            "name": "US_WALTHAM",  
            "label": "Waltham (USA)"  
        }  
    ]  
}
```

[Example Value](#) | [Schema](#)

{}

API Access Tokens

Before using the Cloud Insights API, you must create one or more **API Access Tokens**. Access tokens are used for specified API types, and can grant read and/or write permissions. You can also set the expiration for each access token. All APIs under the specified types are valid for the access token. Each token is void of a username or password.

To create an Access Token:

- Click **Admin > API Access**
- Click **+API Access Token**
 - Enter Token Name
 - Select API Types
 - Specify the permissions granted for this API access
 - Specify Token Expiration

Your token will only be available for copying to the clipboard and saving during the creation process. Tokens can not be retrieved after they are created, so it is highly recommended to copy the token and save it in a secure location. You will be prompted to click the **Copy API Access Token** button before you can close the token creation screen.



You can disable, enable, and revoke tokens. Tokens that are disabled can be enabled.

Tokens grant general purpose access to APIs from a customer perspective; managing access to APIs in the scope of their own tenant. Customer administrators may grant and revoke these tokens without direct involvement from Cloud Insights back end personnel.

The application receives an Access Token after a user successfully authenticates and authorizes access, then passes the Access Token as a credential when it calls the target API. The passed token informs the API that the bearer of the token has been authorized to access the API and perform specific actions specified by the scope that was granted during authorization.

The HTTP header where the Access Token is passed is **X-CloudInsights-ApiKey**:

For example, use the following to retrieve storages assets:

```
curl https://<tenant_host_name>/rest/v1/assets/storages -H 'X-CloudInsights-ApiKey: <API_Access_Token>'
```

Where *<API_Access_Token>* is the token you saved during API access creation.

API Type

The Cloud Insights API is category-based, and currently contains the following types:

- ASSETS type contains asset, query, and search APIs.
 - Assets: Enumerate top-level objects and retrieve a specific object or an object hierarchy.
 - Query: Retrieve and manage Cloud Insights queries.
 - Import: Import annotations or applications and assign them to objects
 - Search: Locate a specific object without knowing the object's unique ID or full name.
- DATA COLLECTION type is used to retrieve and manage data collectors.
- DATA INGESTION type is used to retrieve and manage ingestion data and custom metrics, such as from Telegraf agents
- LOG INGESTION is used to retrieve and manage log data

Additional types and/or APIs may become available over time. You can find the latest API information in the [API Swagger documentation](#).

Note that the API types to which a user has access depend also on the [User Role](#) they have in each Cloud Insights feature set (Monitoring, Workload Security, Reporting).

Inventory Traversal

This section describes how to traverse a hierarchy of Cloud Insights objects.

Top Level Objects

Individual objects are identified in requests by unique URL (called “self” in JSON) and require knowledge of object type and internal id. For some of the top level objects (Hosts, Storages, and so on), REST API provides

access to the complete collection.

The general format of an API URL is:

```
https://<tenant>/rest/v1/<type>/<object>
```

For example, to retrieve all storages from a tenant named *mysite.c01.cloudinsights.netapp.com*, the request URL is:

```
https://mysite.c01.cloudinsights.netapp.com/rest/v1/assets/storages
```

Children and Related Objects

Top level objects, such as Storage, can be used to traverse to other children and related objects. For example, to retrieve all disks for a specific storage, concatenate the storage “self” URL with “/disks”, for example:

```
https://<tenant>/rest/v1/assets/storages/4537/disks
```

Expands

Many API commands support the **expand** parameter, which provides additional details about the object or URLs for related objects.

The one common expand parameter is *expands*. The response contains a list of all available specific expands for the object.

For example, when you request the following:

```
https://<tenant>/rest/v1/assets/storages/2782?expand=_expands
```

The API returns all available expands for the object as follows:

```
{  
    "id": "1247936",  
    "self": "/rest/v1/assets/storages/1247936",  
    "name": "amsprdclu01",  
    "simpleName": "amsprdclu01",  
    "naturalKey": "5DF483F0-1729-11DC-9A79-123478563412",  
    "ip": "10.64.0.132",  
    "serialNumber": "1-80-000011",  
    "model": "FAS3270,FAS6290",  
    "vendor": "NetApp",  
    "microcodeVersion": "8.1.3 clustered Data ONTAP",  
    "capacity": {  
        "description": "Storage Capacity",  
        "unitType": "MB",  
        "total": {  
            "value": 8.23185105E8  
        },  
        "storagePools": {  
            "value": 5.43220974E8  
        }  
    },  
    "isActive": true,  
    "createTime": "2013-05-07T16:52:21-0700",  
    "family": "FAS3200,FAS6200",  
    "managementUrl": null,  
    "virtualizedType": "STANDARD",  
    "protocols": [  
        "NAS",  
        "NFS",  
        "CIFS",  
        "FC",  
        "ISCSI"  
    ],  
    "_expands": {  
        "performance": {  
            "url": "/rest/v1/assets/storages/1247936/performance",  
            "name": "Performance Data"  
        },  
        "storageNodes": {  
            "url": "/rest/v1/assets/storages/1247936/storageNodes",  
            "name": "Storage Storage Nodes"  
        },  
        "storagePools": {  
            "url": "/rest/v1/assets/storages/1247936/storagePools",  
            "name": "Storage Storage Pools"  
        },  
        "storageResources": {  
            "url": "/rest/v1/assets/storages/1247936/storageResources",  
            "name": "Storage Storage Resources"  
        },  
        "internalVolumes": {  
            "url": "/rest/v1/assets/storages/1247936/internalVolumes",  
            "name": "Storage Internal Volumes"  
        },  
        "volumes": {  
            "url": "/rest/v1/assets/storages/1247936/volumes",  
            "name": "Storage Volumes"  
        },  
        "disks": {  
            "url": "/rest/v1/assets/storages/1247936/disks",  
            "name": "Disks"  
        },  
        "datasources": {  
            "url": "/rest/v1/assets/storages/1247936/datasources",  
            "name": "Storage Datasources"  
        },  
        "ports": {  
            "url": "/rest/v1/assets/storages/1247936/ports",  
            "name": "Storage Ports"  
        },  
        "annotations": {  
            "url": "/rest/v1/assets/storages/1247936/annotations",  
            "name": "Storage Annotations"  
        },  
        "qtrees": {  
            "url": "/rest/v1/assets/storages/1247936/qtrees",  
            "name": "Qtrees"  
        },  
        ".....  
    }  
}
```

Each expand contains data, a URL, or both. The expand parameter supports multiple and nested attributes, for example:

```
https://<tenant>/rest/v1/assets/storages/2782?expand=performance,storageResources.storage
```

Expand allows you to bring in a lot of related data in one response. NetApp advises that you do not request too much information at one time; this can cause performance degradation.

To discourage this, requests for top-level collections cannot be expanded. For example, you cannot request expand data for all storage objects at once. Clients are required to retrieve the list of objects and then choose specific objects to expand.

Performance Data

Performance data is gathered across many devices as separate samples. Every hour (the default), Cloud Insights aggregates and summarizes performance samples.

The API allows access to both the samples and the summarized data. For an object with performance data, a performance summary is available as `expand=performance`. Performance history time series are available through nested `expand=performance.history`.

Examples of Performance Data objects include:

- StoragePerformance
- StoragePoolPerformance
- PortPerformance
- DiskPerformance

A Performance Metric has a description and type and contains a collection of performance summaries. For example, Latency, Traffic, and Rate.

A Performance Summary has a description, unit, sample start time, sample end time, and a collection of summarized values (current, min, max, avg, etc.) calculated from a single performance counter over a time range (1 hour, 24 hours, 3 days, and so on).

<https://tenant.cloudinsights.netapp.com/rest/v1/assets/storages/1/performance?expand=history>

Details

Response body

```
{  
    "self": "/rest/v1/assets/storages/1/performance", ← Self  
    "cacheHitRatio": { ← Performance Metric  
        "read": {  
            "description": "Cache Hit Ratio - Read",  
            "unitType": "%",  
            "start": null,  
            "end": null,  
            "current": null,  
            "min": null,  
            "max": null,  
            "avg": null,  
            "sum": null,  
            "isDownsampled": false  
        },  
        "write": {  
            "description": "Cache Hit Ratio - Write",  
            "unitType": "%",  
            "start": null,  
            "end": null,  
            "current": null,  
            "min": null,  
            "max": null,  
            "avg": null  
        }  
    },  
    "history": [ ← History  
        [  
            1578418848140, ← Timestamp  
            { ← Counter Values  
                "latency.total": 1.30578,  
                "latency.read": 3.64681,  
                "ioDensity.read": 9.62065,  
                "iops.write": 686.35502,  
                "ioDensity.total": 31.36259,  
                "capacity.raw": 80024.92772,  
                "throughput.read": 7.32371,  
                "iops.total": 1488.7974,  
                "latency.write": 0.39495,  
                "ioDensity.write": 14.45856,  
                "iops.read": 456.69703,  
                "capacity.storagePools": 56058.1041,  
                "throughput.write": 14.59581,  
                "throughput.total": 21.91953  
            }  
        ],  
        [  
            1578419748198,  
            {  
                "latency.total": 1.30578,  
                "latency.read": 3.64681,  
                "ioDensity.read": 9.62065,  
                "iops.write": 686.35502,  
                "ioDensity.total": 31.36259,  
                "capacity.raw": 80024.92772,  
                "throughput.read": 7.32371,  
                "iops.total": 1488.7974,  
                "latency.write": 0.39495,  
                "ioDensity.write": 14.45856,  
                "iops.read": 456.69703,  
                "capacity.storagePools": 56058.1041,  
                "throughput.write": 14.59581,  
                "throughput.total": 21.91953  
            }  
        ]  
    ]  
}
```

Response body

```
}  
},  
"history": [ ← History  
    [  
        1578418848140, ← Timestamp  
        { ← Counter Values  
            "latency.total": 1.30578,  
            "latency.read": 3.64681,  
            "ioDensity.read": 9.62065,  
            "iops.write": 686.35502,  
            "ioDensity.total": 31.36259,  
            "capacity.raw": 80024.92772,  
            "throughput.read": 7.32371,  
            "iops.total": 1488.7974,  
            "latency.write": 0.39495,  
            "ioDensity.write": 14.45856,  
            "iops.read": 456.69703,  
            "capacity.storagePools": 56058.1041,  
            "throughput.write": 14.59581,  
            "throughput.total": 21.91953  
        }  
    ],  
    [  
        1578419748198,  
        {  
            "latency.total": 1.30578,  
            "latency.read": 3.64681,  
            "ioDensity.read": 9.62065,  
            "iops.write": 686.35502,  
            "ioDensity.total": 31.36259,  
            "capacity.raw": 80024.92772,  
            "throughput.read": 7.32371,  
            "iops.total": 1488.7974,  
            "latency.write": 0.39495,  
            "ioDensity.write": 14.45856,  
            "iops.read": 456.69703,  
            "capacity.storagePools": 56058.1041,  
            "throughput.write": 14.59581,  
            "throughput.total": 21.91953  
        }  
    ]  
]
```

The resulting Performance Data dictionary has the following keys:

- "self" is the object's unique URL

- “history” is the list of pairs of timestamp and map of counters values
- Every other dictionary key (“diskThroughput” and so on) is the name of a performance metric.

Each performance data object type has a unique set of performance metrics. For example, the Virtual Machine performance object supports “diskThroughput” as a performance metric. Each supported performance metric is of a certain “performanceCategory” presented in the metric dictionary. Cloud Insights supports several performance metric type listed later in this document. Each performance metric dictionary will also have the “description” field that is a human-readable description of this performance metric and a set of performance summary counter entries.

The Performance Summary counter is the summarization of performance counters. It presents typical aggregated values like min, max, and avg for a counter and also the latest observed value, time range for summarized data, unit type for counter and thresholds for data. Only thresholds are optional; the rest of attributes are mandatory.

Performance summaries are available for these types of counters:

- Read – Summary for read operations
- Write – Summary for write operations
- Total – Summary for all operations. It may be higher than the simple sum of read and write; it may include other operations.
- Total Max – Summary for all operations. This is the maximum total value in the specified time range.

Object Performance Metrics

The API can return detailed metrics for objects in your environment, for example:

- Storage Performance Metrics such as IOPS (Number of input/output requests per second), Latency, or Throughput.
- Switch Performance Metrics, such as Traffic Utilization, BB Credit Zero data, or Port Errors.

See the [API Swagger documentation](#) for information on metrics for each object type.

Performance History Data

History data is presented in performance data as a list of timestamp and counter maps pairs.

History counters are named based on the performance metric object name. For example, the virtual machine performance object supports “diskThroughput” so the history map will contain keys named “diskThroughput.read”, “diskThroughput.write” and “diskThroughput.total”.



Timestamp is in UNIX time format.

The following is an example of a performance data JSON for a disk:

```

"performance": {
    "self": "/rest/v1/assets/disks/4013931/performance",
    "iops": {
        "performanceCategory": "IOPS",
        "description": "Disk IOPS",
        "read": {
            "description": "Disk Read Iops",
            "unitType": "IO/s",
            "start": 1399305599999,
            "end": 1402604368055,
            "current": 1,
            "min": 0,
            "max": 6,
            "avg": 0.5532
        },
        [...]
    },
    "total": {
        "description": "Disk Total Throughput",
        "unitType": "MB/s",
        "start": 1399305599999,
        "end": 1402604368055,
        "current": 0,
        "min": 0,
        "max": 2,
        "avg": 0.1702
    }
},
"history": [
    [
        1399300412690,
        {
            "utilization.total": 12,
            "iops.total": 26,
            "iops.write": 22,
            "iops.read": 4,
            "throughput.read": 0,
            "utilization.read": 2.12,
            "throughput.total": 5,
            "utilization.write": 10.24,
            "throughput.write": 5
        }
    ]
]
}

```

Objects with Capacity Attributes

Objects with capacity attributes use basic data types and the CapacityItem for representation.

CapacityItem

CapacityItem is a single logical unit of capacity. It has “value” and “highThreshold” in units defined by its parent object. It also supports an optional breakdown map that explains how the capacity value is constructed. For example, the total capacity of a 100 TB storagePool would be a CapacityItem with a value of 100. The breakdown may show 60 TB allocated for “data” and 40 TB for “snapshots”.

Note

“highThreshold” represents system defined thresholds for the corresponding metrics, which a client can use to generate alerts or visual cues on values that are out of acceptable configured ranges.

The following shows the capacity for StoragePools with multiple capacity counters:

StoragePoolCapacity

```
Model properties:  
{  
    description: string  
    unitType: 'MB' or 'GB' or 'TB' or 'KiB' or 'MiB' or 'TiB'  
    total: CapacityItem  
    used: CapacityItem  
    provisioned: CapacityItem  
    reservedCapacity: CapacityItem  
    softLimit: Double  
    rawToUsableRatio: Double  
    isDedupeEnabled: boolean  
    dedupeSavings: NumericValueWithUnit  
    isCompressionEnabled: boolean  
    compressionSavings: NumericValueWithUnit  
    isThinProvisioningSupported: boolean  
}
```

[close](#)

Using Search to Look Up Objects

The search API is a simple entry point to the system. The only input parameter to the API is a free-form string and the resulting JSON contains a categorized list of results. Types are different asset types from the Inventory, such as storages, hosts, dataStores, and so on. Each type would contain a list of objects of the type that match the search criteria.

Cloud Insights is an extensible (wide open) solution that allows integrations with third party orchestration, business management, change control and ticketing systems as well as custom CMDB integrations.

Cloud Insights RESTful API is a primary point of integration that allows simple and effective movement of data as well as allows users to gain seamless access to their data.

Disabling or Revoking an API Token

To temporarily disable an API token, on the API token list page, click the "three dots" menu for the API, and select *Disable*. You can Re-enable the token at any time using the same menu and selecting *Enable*.

To permanently remove an API token, from the menu, select "Revoke". You cannot re-enable a revoked token; you must create a new token.

API Access Tokens (252) ?						
<input type="checkbox"/>	Name ↑	Description	Token	API Type	Permission	Expires On
<input type="checkbox"/>	10.197.120.70		...RpTMJ4	Data Ingestion	Write Only	11/06/2021 Expired
	22		...nUBDhe	Data Ingestion	Write Only	06/17/2022 Enabled
	22TOKEN2010560		...8gXq7K	All Categories	Read Only	06/17/2022 Enabled
	ActiveIQ_POC_token		...scmES6	Data Ingestion	Read/Write	11/12/2021 Expired

[+ API Access Token](#) [Bulk Actions](#) [Filter...](#) [?](#)

...
[Disable](#)
[Edit Description](#)
[Revoke](#)

Rotating Expired API Access Tokens

API access tokens have an expiration date. When an API access token expires, users need to generate a new token (of type *Data Ingestion* with Read/Write permissions) and reconfigure Telegraf to use the newly-generated token instead of the expired token. The steps below detail how to do this.

Kubernetes

Note that these commands are using the default namespace "netapp-monitoring". If you have set your own namespace, substitute that namespace in these and all subsequent commands and files.

Note: If you have the latest NetApp Kubernetes Monitoring Operator installed and using an API access token that is renewable, expiring tokens will automatically be replaced by new/refreshed API access tokens. There is no need to perform the manual steps listed below.

- Edit the the NetApp Kubernetes Monitoring Operator.

```
kubectl -n netapp-monitoring edit agent agent-monitoring-netapp
```

- Modify the *spec.output-sink.api-key* value, replacing the old API token with the new API token.

```
spec:  
...  
  output-sink:  
    - api-key: <NEW_API_TOKEN>
```

RHEL/CentOS and Debian/Ubuntu

- Edit the Telegraf configuration files, and replace all instances of the old API token with the new API token.

```
sudo sed -i.bkup 's/<OLD_API_TOKEN>/<NEW_API_TOKEN>/g'  
/etc/telegraf/telegraf.d/*.conf
```

- Restart Telegraf.

```
sudo systemctl restart telegraf
```

MacOS

- Edit the Telegraf configuration files, and replace all instances of the old API token with the new API token.

```
sudo sed -i.bkup 's/<OLD_API_TOKEN>/<NEW_API_TOKEN>/g'  
/usr/local/etc/telegraf.d/*.conf
```

- Restart Telegraf.

```
sudo launchctl stop telegraf  
sudo launchctl start telegraf
```

Windows

- For each Telegraf configuration file in *C:\Program Files\telegraf\telegraf.d*, replace all instances of the old API token with the new API token.

```
cp <plugin>.conf <plugin>.conf.bkup  
(Get-Content <plugin>.conf).Replace('<OLD_API_TOKEN>',  
'<NEW_API_TOKEN>') | Set-Content <plugin>.conf
```

- Restart Telegraf.

```
Stop-Service telegraf  
Start-Service telegraf
```

Notification using Webhooks

Webhooks allow users to send alert notifications to various applications using a customized webhook channel.

Many commercial applications support webhooks as a standard input interface, for example: Slack, PagerDuty, Teams, and Discord all support webhooks. By supporting a generic, customizable webhook channel, Cloud Insights can support many of these delivery channels. Information on webhooks can be found on these application websites. For example, Slack provides [this useful guide](#).

You can create multiple webhook channels, each channel targeted for a different purpose; separate applications, different recipients, etc.

The webhook channel instance is comprised of the following elements:

Name	Unique name
URL	Webhook target URL, including the <i>http://</i> or <i>https://</i> prefix along with the url params
Method	GET, POST - Default is POST
Custom Header	Specify any custom header lines here
Message Body	Put the body of your message here
Default Alert Parameters	Lists the default parameters for the webhook
Custom Parameters and Secrets	Custom parameters and secrets allow you to add unique parameters and secure elements such as passwords

Creating a Webhook

To create a Cloud Insights webhook, go to **Admin > Notifications** and select the **Webhooks** tab.

The following image shows an example webhook configured for Slack:

Edit a Webhook

Name

Template Type

URL

Method

Custom Header

```
Content-Type: application/json  
Accept: application/json
```

Message Body

```
{
  "blocks": [
    {
      "type": "section",
      "text": {
        "type": "mrkdwn",
        "text": "*Cloud Insights Alert - %%alertId%%*\nSeverity - *%%severity%%*"
      }
    }
  ]
}
```

Enter appropriate information for each of the fields, and click "Save" when complete.

You can also click the "Test Webhook" button to test the connection. Note that this will send the "Message Body" (without substitutions) to the defined URL according to the selected Method.

Cloud Insights webhooks comprise a number of default parameters. Additionally, you can create your own custom parameters or secrets.

Default Alert Parameters

Name	Description
%%alertDescription%%	Alert description
%%alertId%%	Alert ID
%%alertRelativeUrl%%	Relative URL to the Alert page. To build alert link use https://%%cloudInsightsHostName%%/%%alertRelativeUrl%%
%%metricName%%	Monitored metric
%%monitorName%%	Monitor name
%%objectType%%	Monitored object type
%%severity%%	Alert severity level
%%alertCondition%%	Alert condition
%%triggerTime%%	Alert trigger time in GMT ('Tue, 27 Oct 2020 01:20:30 GMT')
%%triggerTimeEpoch%%	Alert trigger time in Epoch format (milliseconds)
%%triggeredOn%%	Triggered On (key:value pairs separated by commas)
%%value%%	Metric value that triggered the alert
%%cloudInsightsLogoUrl%%	Cloud Insights logo URL
%%cloudInsightsHostname%%	Cloud Insights Hostname (concatenate with relative URL to build alert link)

Custom Parameters and Secrets i

Name	Value	Description
No Data Available		
+ Parameter		

Parameters: What are they and how do I use them?

Alert Parameters are dynamic values populated per alert. For example, the %%TriggeredOn%% parameter will be replaced with the object on which the alert was triggered.

Note that in this section, substitutions are *not* performed when clicking the "Test Webhook" button; the button sends a payload that shows the %% substitutions but does not replace them with data.

Custom Parameters and Secrets

In this section you can add any custom parameters and/or secrets you wish. For security reasons, if a secret is defined only the webhook creator can modify this webhook channel. It is read-only for others. You can use secrets in URL/Headers as %%<secret_name>%%.

Choosing Webhook Notification in a Monitor

To choose the webhook notification in a [monitor](#), go to **Alerts > Manage Monitors** and select the desired monitor, or add a new monitor. In the *Set up team notifications* section, choose *Webhook* as the delivery method. Select the alert levels (Critical, Warning, Resolved), then choose the desired webhook.

3 Set up team notification(s) (alert your team via email, or Webhook)

The screenshot shows a user interface for configuring team notifications. On the left, there's a section labeled "By Webhook" with a dropdown menu set to "Notify team on: Critical, Warning, Resolved". To the right, there's a section labeled "Use Webhook" with a dropdown menu that is currently open. The open menu has a search bar at the top with the placeholder "Search...". Below the search bar, there are two listed options: "ci-alerts-notifications-dev" and "ci-alerts-notifications-qa".

Webhook Examples:

- Webhooks for [Slack](#)
- Webhooks for [PagerDuty](#)
- Webhooks for [Teams](#)
- Webhooks for [Discord](#)

Monitoring your Environment

Auditing

To identify changes both expected (for tracking) or unexpected (for troubleshooting), you can view an audit trail of the Cloud Insights system events and user activities.

Viewing Audited Events

To View the Audit page, click **Admin > Audit** in the menu. The Audit page is displayed, providing the following details for each audit entry:

- **Time** - Date and time of the event or activity
- **User** - The User who initiated the activity
- **Role** - The user's role in Cloud Insights (guest, user, administrator)
- **IP** - The IP address associated with the event
- **Action** - Type of activity, for example Login, Create, Update
- **Category** - The category of activity
- **Details** - Details of the activity

Displaying audit entries

There are a number of different ways to view audit entries:

- You can display audit entries by choosing a particular time period (1 hour, 24 hours, 3 days, etc.).
- You can change the sort order of entries to either ascending (up arrow) or descending (down arrow) by clicking the arrow in the column header.

By default, the table displays the entries in descending time order.

- You can use the filter fields to show only the entries you want in the table. Click the [+] button to add additional filters.

The screenshot shows a table titled "Audit (15)" with columns: Time, User, Role, and IP. A filter dialog is open over the table, specifically for the "Action" column. The dialog lists several options: Create, Delete, Update, Enable, Disable, and Accept. The "Create", "Delete", and "Update" checkboxes are checked, while the others are unchecked. The "Any" checkbox at the top of the dialog is also checked.

Time	User	Role	IP
12/09/2020 10:16:42 AM	Tony Lavoie	admin	216.240.10.25

More on Filtering

You can use any of the following to refine your filter:

Filter	What it does	Example	Result
* (Asterisk)	enables you to search for everything	vol*rhel	returns all resources that start with "vol" and end with "rhel"
? (question mark)	enables you to search for a specific number of characters	BOS-PRD??-S12	returns BOS-PRD12-S12, BOS-PRD23-S12, and so on
OR	enables you to specify multiple entities	FAS2240 OR CX600 OR FAS3270	returns any of FAS2440, CX600, or FAS3270
NOT	allows you to exclude text from the search results	NOT EMC*	returns everything that does not start with "EMC"
None	searches for blank/NULL/None in any field where selected	None	returns results where the target field is not empty
Not *	as with None above, but you can also use this form to search for NULL values in <i>text-only</i> fields	Not *	returns results where the target field is not empty.
""	searches for an exact match	"NetApp*"	returns results containing the exact literal string NetApp*

If you enclose a filter string in double quotes, Insight treats everything between the first and last quote as an exact match. Any special characters or operators inside the quotes will be treated as literals. For example, filtering for "*" will return results that are a literal asterisk; the asterisk will not be treated as a wildcard in this case. The operators OR and NOT will also be treated as literal strings when enclosed in double quotes.

Audited Events and Actions

The events and actions audited by Cloud insights can be categorized in the following broad areas:

- **User account:** Log in, log out, role change, etc.

Example: *User Tony Lavoie logged in from 10.1.120.15, user agent Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36, login method(s) Cloud Central Portal Login*

- **Acquisition Unit:** create, delete, etc.

Example: *Acquisition unit AU-Boston-1 removed.*

- **Data Collector:** add, remove, modify, postpone/resume, change acquisition unit, start/stop, etc.

Example: *Datasource FlexPod Lab removed, vendor NetApp, model ONTAP Data Management Software, ip 192.168.106.5.*

- **Application:** add, assign to object, remove, etc.

Example: *Internal Volume **ocisedev:t1appSVM01:t1appFlexVol01** added to application **Test App**.*

- **Annotation:** add, assign, remove, annotation rule actions, annotation value changes, etc.

Example: *Annotation value **Boston** added to annotation type **SalesOffice**.*

- **Query:** add, remove, etc.

Example: *Query **TL Sales Query** is added.*

- **Monitor:** add, remove, etc.

Example: *Monitor Aggr Size - CI Alerts Notifications Dev updated*

- **Notification:** change email, etc.

Example: *Recipient **ci-alerts-notifications-dl** created*

Exporting Audit Events

You can export the results of your Audit display to a .CSV file, which will allow you to analyze the data or import it into another application.

Steps

1. On the Audit page, set the desired time range and any filters you want. Cloud Insights will export only the Audit entries that match the filtering and time range you have set.
2. Click the *Export* button  in the upper right of the table.

The displayed Audit events will be exported to a .CSV file, up to a maximum of 10,000 rows.

Retention of Audit Data

The amount of time Cloud Insights retains Audit data is based on your Edition:

- Basic Edition: Audit data is retained for 30 days
- Standard and Premium Editions: Audit data is retained for 1 year plus 1 day

Audit entries older than the retention time are automatically purged. No user interaction is needed.

Troubleshooting

Here you will find suggestions for troubleshooting problems with Audit.

Problem:	Try this:
I see Audit messages telling me that a monitor has been exported.	Export of a custom monitor configuration is typically used by NetApp engineers during development and testing of new features. If you did not expect to see this message, please consider exploring the actions of the user named in the audited action or contact support.

Asset Page Information

Asset Page Overview

Asset pages summarize the current status of an asset and contain links to additional information about the asset and its related assets.

Types of Asset Pages

Cloud Insights provides asset pages for the following assets:

- Virtual machine
- Storage Virtual Machine (SVM)
- Volume
- Internal volume
- Host (including Hypervisor)
- Storage pool
- Storage
- Datastore
- Application
- Storage node
- Qtree
- Disk
- VMDK
- Port
- Switch
- Fabric

Changing the Time Range of Displayed Data

By default, an asset page displays the last 24 hours of data; however, you can change the segment of data displayed by selecting another fixed time range or a custom range of time to view less or more data.

You can change the time segment of displayed data by using an option that is located on every asset page, regardless of asset type. To change the time range, click the displayed time range in the top bar and choose from among the following time segments:

- Last 15 Minutes
- Last 30 Minutes
- Last 60 Minutes
- Last 2 Hours
- Last 3 Hours (this is the default)
- Last 6 Hours

- Last 12 Hours
- Last 24 Hours
- Last 2 Days
- Last 3 Days
- Last 7 Days
- Last 30 Days
- Custom time range

The Custom time range allows you to select up to 31 consecutive days. You can also set the Start Time and End Time of day for this range. The default Start Time is 12:00 AM on the first day selected and the default End Time is 11:59 PM on the last day selected. Clicking Apply will apply the custom time range to the asset page.

Add Custom Widgets

You can add your own widgets to any asset page. Widgets you add will appear on asset pages for all objects of that type. For example, adding a custom widget to a storage asset page will display that widget on asset pages for all storage assets.

Filtering for Objects In-Context

When configuring a widget on an asset's landing page, you can set *in-context* filters to show only objects directly related to the current asset. By default, when you add a widget, *all* objects of the selected type in your environment are displayed. In-context filters allow you to display only the data relevant to your current asset.

On most asset landing pages, widgets allow you to filter for objects related to the current asset. In filter dropdowns, object types that display a link icon  can be filtered in-context to the current asset.

For example, on a Storage asset page, you can add a Bar Chart widget to show the top IOPS on internal volumes only on that storage. By default, when you add a widget, *all* internal volumes in your environment are displayed.

To show only internal volumes on the current storage asset, do the following:

Steps

1. Open an asset page for any **Storage** asset.
2. Click **Edit** to open the asset page in Edit mode.
3. Click **Add Widget** and select *Bar Chart*.
4. Select **Internal Volume** for the object type to display on the bar chart. Notice that the internal volume object type has a link icon  beside it. The "linked" icon is enabled by default.



5. Choose *IOPS - Total* and set any additional filters you like.
6. Collapse the **Roll Up** field by clicking the [X] beside it. The **Show** field is displayed.
7. Choose to show Top 10.
8. Save the widget.

The bar chart shows only the internal volumes that reside on the current storage asset.

The widget will be displayed on the asset pages for all storage objects. When the in-context link is enabled in the widget, the bar chart shows data for internal volumes related only to the currently-displayed storage asset.

To unlink the object data, edit the widget and click the link icon next to the object type. The link becomes disabled and the chart displays data for *all* objects in your environment.

You can also use [special variables in widgets](#) to display asset-related information on landing pages.

Asset Page Summary section

The Summary section of an asset page displays general information about an asset, including whether any metrics or performance policies are cause for concern. Potential problem areas are indicated by a red circle.

Virtual Machine Summary

C 5m

Power State: On	Latency - Total: 6.35 ms	Hypervisor Name: us-east-1a
Guest State: Running	IOPS - Total: ! 316.59 IO/s	Hypervisor IP: US-EAST-1A-052113251141
Datastore: i-00cc58b5c47a69271	Throughput - Total: 68.81 MB/s	Hypervisor OS: Amazon AWS EC2
CPU Utilization - Total: 13.82 %	DNS Name: ip-10-30-23-12.ec2.internal	Hypervisor FC Fabrics: 0
Memory Utilization - Total: N/A	IP: 10.30.23.12	Hypervisor CPU Utilization: N/A
Memory: 32.0 GB	OS: CentOS Linux 7 x86_64 HVM EBS ENA 1901_01-b7ee8a69- ee97-4a49-9e68-afaaee216db2e- ami-05713873c6794f575.4 x86_64	Hypervisor Memory Utilization: N/A
Capacity - Total: 200.0 GB	Processors: 8	Alert Monitors: High Latency VMs Instance CPU Under-utilized
Capacity - Used: N/A		View Topology

Note: The information displayed in the Summary section varies, depending on the type of asset you are viewing.

You can click any of the asset links to view their asset pages. For example, if you are viewing a storage node, you can click a link to view the asset page of the storage it is associated with.

You can view the metrics associated with the asset. A red circle next to a metric indicates that you might need to diagnose and resolve potential problems.



You may notice that volume capacity might show greater than 100% on some storage assets. This is due to metadata related to the capacity of the volume being part of the consumed capacity data reported by the asset.

If applicable, you can click an alert link to view the alert and monitor associated with the asset.

Topology

On certain asset pages, the summary section contains a link to view the topology of the asset and its connections.

Topology is available for the following asset types:

- Application
- Disk
- Fabric
- Host
- Internal Volume
- Port
- Switch
- Virtual Machine
- VMDK
- Volume

Internal Volume

Storage:	barbados1,barbados2	Latency - Total:	0.02 ms
Storage Pool:	barbados1:agg1	Storage Pool Utilization:	0.68 %
Status:	Online	IOPS - Total:	0.13 IO/s
Type:	FlexVol	Datastore:	
UUID:		Deduplication Savings:	0.0 %
SVM/Filer:	vfiler0	Thin Provisioned:	No
Capacity - Total:	1.0 GB	Replication Source(s):	
Capacity - Used:	0.0 GB	Performance Policies:	Find High Latency FlexVols
Snapshot:	<0.1 GB		

[View Topology](#)

Topology

```

graph LR
    H((H)) --> NAS[NAS]
    NAS --> S((S))
    
```

[Close](#)

Expert View

The Expert View section of an asset page enables you to view a performance sample for the base asset based on any number of applicable metrics in context with a chosen time period in the performance chart and any assets related to it.

Using the Expert View section

The following is an example of the Expert View section in a storage asset page:



You can select the metrics you want to view in the performance chart for the time period selected. Click on the **Display Metrics** drop-down and choose from the metrics listed.

The **Resources** section shows the name of the base asset and the color representing the base asset in the performance chart. If the **Top Correlated** section does not contain an asset you want to view in the performance chart, you can use the **Search Assets** box in the **Additional Resources** section to locate the asset and add it to the performance chart. As you add resources, they appear in the Additional resources section.

Also shown in the Resources section, when applicable, are any assets related to the base asset in the following categories:

- Top correlated

Shows the assets that have a high correlation (percentage) with one or more performance metrics to the base asset.

- Top contributors

Shows the assets that contribute (percentage) to the base asset.

- Workload Contentions

Shows the assets that impact or are impacted by other shared resources, such as hosts, networks, and storage. These are sometimes called *greedy* and *degraded* resources.

Alerts in Expert View

Alerts are also displayed in the Expert View section of an asset landing page, showing the time and duration of the alert as well as the monitor condition that triggered it.



Expert View metric definitions

The Expert View section of an asset page displays several metrics based on the time period selected for the asset. Each metric is displayed in its own performance chart. You can add or remove metrics and related assets from the charts depending on what data you want to see. The metrics you can choose will vary depending on asset type.

Metric	Description
BB credit zero Rx, Tx	Number of times the receive/transmit buffer-to-buffer credit count transitioned to zero during the sampling period. This metric represents the number of times the attached port had to stop transmitting because this port was out of credits to provide.
BB credit zero duration Tx	Time in milliseconds during which the transmit BB credit was zero during the sampling interval.
Cache hit ratio (Total, Read, Write) %	Percentage of requests that result in cache hits. The higher the number of hits versus accesses to the volume, the better is the performance. This column is empty for storage arrays that do not collect cache hit information.
Cache utilization (Total) %	Total percentage of cache requests that result in cache hits
Class 3 discards	Count of Fibre Channel Class 3 data transport discards.
CPU utilization (Total) %	Amount of actively used CPU resources, as a percentage of total available (over all virtual CPUs).
CRC error	Number of frames with invalid cyclic redundancy checks (CRCs) detected by the port during the sampling period
Frame rate	Transmit frame rate in frames per second (FPS)
Frame size average (Rx, Tx)	Ratio of traffic to frame size. This metric enables you to identify whether there are any overhead frames in the fabric.
Frame size too long	Count of Fibre Channel data transmission frames that are too long.

Frame size too short	Count of Fibre Channel data transmission frames that are too short.
I/O density (Total, Read, Write)	Number of IOPS divided by used capacity (as acquired from the most recent inventory poll of the data source) for the Volume, Internal Volume or Storage element. Measured in number of I/O operations per second per TB.
IOPS (Total, Read, Write)	Number of read/write I/O service requests passing through the I/O channel or a portion of that channel per unit of time (measured in I/O per sec)
IP throughput (Total, Read, Write)	Total: Aggregated rate at which IP data was transmitted and received in megabytes per second.
Read: IP Throughput (Receive):	Average rate at which IP data was received in megabytes per second.
Write: IP Throughput (Transmit):	Average rate at which IP data was transmitted in megabytes per second.
Latency (Total, Read, Write)	Latency (R&W): Rate at which data is read or written to the virtual machines in a fixed amount of time. The value is measured in megabytes per second.
Latency:	Average response time from the virtual machines in a data store.
Top Latency:	The highest response time from the virtual machines in a data store.
Link failure	Number of link failures detected by the port during the sampling period.
Link reset Rx, Tx	Number of receive or transmit link resets during the sampling period. This metric represents the number of link resets that were issued by the attached port to this port.
Memory utilization (Total) %	Threshold for the memory used by the host.
Partial R/W (Total) %	Total number of times that a read/write operation crosses a stripe boundary on any disk module in a RAID 5, RAID 1/0, or RAID 0 LUN. Generally, stripe crossings are not beneficial, because each one requires an additional I/O. A low percentage indicates an efficient stripe element size and is an indication of improper alignment of a volume (or a NetApp LUN). For CLARiiON, this value is the number of stripe crossings divided by the total number of IOPS.
Port errors	Report of port errors over the sampling period/given time span.
Signal loss count	Number of signal loss errors. If a signal loss error occurs, there is no electrical connection, and a physical problem exists.

Swap rate (Total Rate, In rate, Out rate)	Rate at which memory is swapped in, out, or both from disk to active memory during the sampling period. This counter applies to virtual machines.
Sync loss count	Number of synchronization loss errors. If a synchronization loss error occurs, the hardware cannot make sense of the traffic or lock onto it. All the equipment might not be using the same data rate, or the optics or physical connections might be of poor quality. The port must resynchronize after each such error, which impacts system performance. Measured in KB/sec.
Throughput (Total, Read, Write)	Rate at which data is being transmitted, received, or both in a fixed amount of time in response to I/O service requests (measured in MB per sec).
Timeout discard frames - Tx	Count of discarded transmit frames caused by timeout.
Traffic rate (Total, Read, Write)	Traffic transmitted, received, or both received during the sampling period, in mebibytes per second.
Traffic utilization (Total, Read, Write)	Ratio of traffic received/transmitted/total to receive/transmit/total capacity, during the sampling period.
Utilization (Total, Read, Write) %	Percentage of available bandwidth used for transmission (Tx) and reception (Rx).
Write pending (Total)	Number of write I/O service requests that are pending.

Using the Expert View section

The Expert view section enables you to view performance charts for an asset based on any number of applicable metrics during a chosen time period, and to add related assets to compare and contrast asset and related asset performance over different time periods.

Steps

1. Locate an asset page by doing either of the following:
 - Search for and select a specific asset.
 - Select an asset from a dashboard widget.
 - Query for a set of assets and select one from the results list.

The asset page displays. By default, the performance chart shows two metrics for time period selected for the asset page. For example, for a storage, the performance chart shows latency and total IOPS by default. The Resources section displays the resource name and an Additional resources section, which enables you to search for assets. Depending on the asset, you might also see assets in the Top correlated, Top contributor, Greedy, and Degraded sections. If there are no assets relevant to these sections, they are not displayed.

2. You can add a performance chart for a metric by clicking **Display Metrics** and selecting the metrics you want displayed.

A separate chart is displayed for each metric selected. The chart displays the data for the selected time

period. You can change the time period by clicking on another time period in the top right corner of the asset page, or by zooming in on any chart.

Click on **Display Metrics** to de-select any chart. The performance chart for the metric is removed from Expert View.

3. You can position your cursor over the chart and change the metric data that displays for that chart by clicking any of the following, depending on the asset:

- Read, Write, or Total
- Tx, Rx, or Total

Total is the default.

You can drag your cursor over the data points in the chart to see how the value of the metric changes over the time period selected.

4. In the Resources section, you can add any related assets to the performance charts:

- You can select a related asset in the **Top Correlated**, **Top Contributors**, **Greedy**, and **Degraded** sections to add data from that asset to the performance chart for each selected metric.

After you select the asset, a color block appears next to the asset to denote the color of its data points in the chart.

5. Click on **Hide Resources** to hide the additional resources pane. Click on **Resources** to show the pane.

- For any asset shown, you can click the asset name to display its asset page, or you can click the percentage that the asset correlates or contributes to the base asset to view more information about the asset's relation to the base asset.

For example, clicking the linked percentage next to a top correlated asset displays an informational message comparing the type of correlation that asset has with the base asset.

- If the Top correlated section does not contain an asset you want to display in a performance chart for comparison purposes, you can use the Search assets box in the Additional resources section to locate other assets.

After you select an asset, it displays in the additional resources section. When you no longer want to view information about the asset, click .

User Data Section

The User Data section of an asset page displays and enables you to change any user-defined data such as applications and annotations.

Using the User Data section to assign or modify applications

You can assign applications running in your environment to certain assets (host, virtual machines, volumes, internal volumes, qtrees, and hypervisors). The User Data section enables you to add, change, or remove the applications assigned to an asset. For all of these asset types except for volumes, you can assign more than one application.

Steps

1. Locate an asset page by doing any of the following:

- a. Query for a list of assets and then select one from the list.
- b. On a Dashboard, locate an asset name and click it.
- c. Perform a search and choose an asset from the results.

The asset page displays. The User Data section of the page shows currently-assigned applications or annotations.

To change the application assigned, or to assign an application or additional applications, drop down the **Application** list and select the application(s) you want to assign to the asset. You can type to search for an application, or select one from the list.

To remove an application, drop down the application list and un-check the application.

Using the User Data section to assign or modify annotations

When customizing Cloud Insights to track data for your corporate requirements, you can define specialized notes called annotations, and assign them to your assets. The User Data section of an asset page displays annotations assigned to an asset and also enables you to change the annotations assigned to that asset.

Steps

1. To add an annotation to the asset, in the User Data section of the asset page, click **+Annotation**.
2. Select an annotation from the list.
3. Click Value and do either of the following, depending on type of annotation you selected:
 - a. If the annotation type is list, date, or Boolean, select a value from the list.
 - b. If the annotation type is text, type a value.
4. Click Save.

The annotation is assigned to the asset. You can later filter assets by annotation using a query.

If you want to change the value of the annotation after you assign it, drop down the annotation list and enter a different value.

If the annotation is of list type for which the *Add new values on the fly* option is selected, you can type to add a new value in addition to selecting an existing value.

Asset Page Related Alerts section

You can use the Related Alerts section of an asset page to see any alerts that occur in your environment as a result of a monitor assigned to an asset. Monitors generate alerts based on conditions you set, and enable you to identify the implication and analyze the impact and root cause of the problem in a manner that enables rapid and effective correction.

The following example shows a typical Related Alerts section that displays on an asset page:

Related Alerts

16 items found						
Alert ID	Active Status	Triggered Time ↓	Top Severity	Monitor	Triggered On	Status
AL-146777	Resolved	5 minutes ago Jul 28, 2021 4:01 PM	⚠ Warning	Workload IOPS	workload_volume_name: podAuVol-wid12074	New
AL-146748	Resolved	11 minutes ago Jul 28, 2021 3:55 PM	⚠ Warning	Workload IOPS	workload_volume_name: podAuVol-wid12074	New
AL-146711	Resolved	23 minutes ago Jul 28, 2021 3:43 PM	❗ Critical	Workload IOPS	workload_volume_name: podAuVol-wid12074	New
AL-146704	Resolved	25 minutes ago	⚠ Warning	Workload IOPS	workload_volume_name: podAuVol-wid12074	New

The Related Alerts section enables you to view and manage the alerts that occur in your network as the result of monitor conditions assigned to an asset.

Steps

- Locate an asset page by doing any of the following:
 - Type the name of the asset in the Search area, and then select the asset from the list.
 - In a dashboard widget, click on the name of an asset.
 - Query for a set of assets and select one from the results list.

The asset page displays. The Related Alerts section displays the time the alert was triggered as well as current status of the alert and the monitor that triggered it. You can click the Alert ID to open the landing page for the alert for further investigation.

Prefix and suffix search

As soon as you start typing a search string, the search engine does a prefix and suffix search to find the best match.

Exact matches are given a higher score than a prefix or suffix match. The score is calculated based on the distance of the search term from the actual search result. For example, we have three storages: "aurora", "aurora1", and "aurora11". Searching for "aur" will return all three storages. However, the search result for "aurora" will have the highest score because it has the closest distance to the prefix search string.

The search engine also searches for terms in reverse order, which allows you to perform a suffix search. For example, when you type "345" in the search box, the search engine searches for "345".

The report data available to you is controlled by several things, including the following:

- Login access to the Reporting Portal, which is defined by roles.
- The setup of the Cloud Insights Data Warehouse, which stores the data for the reports.

AWS Cloud Cost Data

The Cloud cost report provides a consolidated view of all assets so you can track, analyze and optimize usage and cost of cloud-based as well as on-prem services as they dynamically scale in your environment.

The report provides infrastructure-to-cost correlation, giving clear and actionable reporting to ensure right-sizing through focused capacity planning and waste detection.

- POST /{schema}/** - Write data and create queries in dwh_custom schema of Data Warehouse database through ODATA protocol, requires ADMIN role

Format: `https://<Cloud Insights URL>/rest/v1/dwh-management/odata/<schema_name>/<table_name>`. The body contains the record in JSON format

Example: add a new record to the storage table: `https://<Cloud Insights URL>/rest/v1/dwh-management/odata/dwh_custom/storage`, Request body: `{"storageId": 123, "storageName": "storage123"}`

Creating queries: POST `https://<Cloud Insights URL>/rest/v1/dwh-management/odata/dwh_custom/custom_queries` -d `{"queryName": "<query_name>", "querySql": "<query_sql>"}`

- PATCH `/{schema}/**` - Modify data and modify queries in dwh_custom schema of Data Warehouse database through ODATA protocol, requires ADMIN role

Format: `https://<Cloud Insights URL>/rest/v1/dwh-management/odata/<schema_name>/<table_name>('<record_id>')`. The body contains the record in JSON format

Example: modify a record in the storage table: `https://<Cloud Insights URL>/rest/v1/dwh-management/odata/dwh_custom/storage('123')`, Request body: `{"storageId": 123, "storageName": "storage123"}`

Modifying queries: PATCH `https://<Cloud Insights URL>/rest/v1/dwh-management/odata/dwh_custom/custom_queries('queryName')` -d `{"queryName": "<query_name>", "querySql": "<query_sql>"}`

- DELETE `/{schema}/**` - Delete data and delete queries in dwh_custom schema of Data Warehouse database through ODATA protocol, requires ADMIN role

Format: `https://<Cloud Insights URL>/rest/v1/dwh-management/odata/<schema_name>/<table_name>('<record_id>')`

Example: delete a record from the storage table: `https://<Cloud Insights URL>/rest/v1/dwh-management/odata/dwh_custom/storage('123')`

Deleting queries: DELETE `https://<Cloud Insights URL>/rest/v1/dwh-management/odata/dwh_custom/custom_queries('queryName')`

Removed from Table:

|Agent outbound URLs (port 433)|

https://<site_name>.cs01.cloudinsights.netapp.com

You can use a broader range to specify the tenant ID: https://*.cs01.cloudinsights.netapp.com/

<https://gateway.c01.cloudinsights.netapp.com>

<https://agentlogin.cs01.cloudinsights.netapp.com>

Files Created During Installation

- Installation directory:

/opt/netapp/cloudsecure/agent

- Installation logs:

/var/log/netapp/cloudsecure/install

/opt/netapp/cloud-secure/logs

- Agent Logs:

- You can use the following command to verify the agent installed correctly:

```
sudo grep -irn register /opt/netapp/cloudsecure/agent/logs/agent.log
```

- Use the following script to uninstall the agent:

```
sudo cloudsecure-agent-uninstall.sh
```

Add to table once link is provided:

For more details about forest names, please refer to this xref:|||||

Enter the following Directory Server required attributes if the default attribute names have been modified in Active Directory. Most often these attributes names are *not* modified in Active Directory, in which case you can simply proceed with the default attribute name.

Attributes	Attribute name in Directory Server
Display Name	name
SID	objectsid
User Name	sAMAccountName

Click Include Optional Attributes to add any of the following attributes:

Attributes	Attribute Name in Directory Server
Email Address	mail
Telephone Number	telephonenumber
Role	title
Country	co
State	state
Department	department

Photo	thumbnailphoto
ManagerDN	manager
Groups	memberOf

Testing Your User Directory Collector Configuration

You can validate LDAP User Permissions and Attribute Definitions using the following procedures:

- Use the following command to validate Workload Security LDAP user permission:

```
ldapsearch -o ldif-wrap=no -LLL -x -b "dc=netapp,dc=com" -h 10.235.40.29 -p 389 -D Administrator@netapp.com -W
```

- Use AD Explorer to navigate an AD database, view object properties and attributes, view permissions, view an object's schema, execute sophisticated searches that you can save and re-execute.
 - Install [AD Explorer](#) on any windows machine which can connect to the AD Server.
 - Connect to the AD server using the username/password of the AD directory server.



Troubleshooting User Directory Collector Configuration Errors

The following table describes known problems and resolutions that can occur during collector configuration:

Problem:	Resolution:
Adding a User Directory connector results in the 'Error' state. Error says, "Invalid credentials provided for LDAP server".	Incorrect username or password provided. Edit and provide the correct user name and password.

Problem:	Resolution:
Adding a User Directory connector results in the 'Error' state. Error says, "Failed to get the object corresponding to DN=DC=hq,DC=domainname,DC=com provided as forest name."	Incorrect forest name provided. Edit and provide the correct forest name.
The optional attributes of domain user are not appearing in the Workload Security User Profile page.	This is likely due to a mismatch between the names of optional attributes added in CloudSecure and the actual attribute names in Active Directory. Edit and provide the correct optional attribute name(s).
Data collector in error state with "Failed to retrieve LDAP users. Reason for failure: Cannot connect on the server, the connection is null"	Restart the collector by clicking on the <i>Restart</i> button.
Adding a User Directory connector results in the 'Error' state.	Ensure you have provided valid values for the required fields (Server, forest-name, bind-DN, bind-Password). Ensure bind-DN input is always provided as 'Administrator@<domain_forest_name>' or as a user account with domain admin privileges.
Adding a User Directory connector results in the 'RETRYING' state. Shows error "Unable to define state of the collector, reason Tcp command [Connect(localhost:35012,None,List(),Some(,seconds),true)] failed because of java.net.ConnectionException:Connection refused."	Incorrect IP or FQDN provided for the AD Server. Edit and provide the correct IP address or FQDN.
Adding a User Directory connector results in the 'Error' state. Error says, "Failed to establish LDAP connection".	Incorrect IP or FQDN provided for the AD Server. Edit and provide the correct IP address or FQDN.
Adding a User Directory connector results in the 'Error' state. Error says, "Failed to load the settings. Reason: Datasource configuration has an error. Specific reason: /connector/conf/application.conf: 70: ldap.Idap-port has type STRING rather than NUMBER"	Incorrect value for Port provided. Try using the default port values or the correct port number for the AD server.
I started with the mandatory attributes, and it worked. After adding the optional ones, the optional attributes data is not getting fetched from AD.	This is likely due to a mismatch between the optional attributes added in CloudSecure and the actual attribute names in Active Directory. Edit and provide the correct mandatory or optional attribute name.
After restarting the collector, when will the AD sync happen?	AD sync will happen immediately after the collector restarts. It will take approximately 15 minutes to fetch user data of approximately 300K users, and is refreshed every 12 hours automatically.
User Data is synced from AD to CloudSecure. When will the data be deleted?	User data is retained for 13months in case of no refresh. If the tenant is deleted then the data will be deleted.

Problem:	Resolution:
<p>User Directory connector results in the 'Error' state. "Connector is in error state. Service name: usersLdap. Reason for failure: Failed to retrieve LDAP users. Reason for failure: 80090308: LdapErr: DSID-0C090453, comment: AcceptSecurityContext error, data 52e, v3839"</p>	<p>Incorrect forest name provided. See above on how to provide the correct forest name.</p>
<p>Telephone number is not getting populated in the user profile page.</p>	<p>This is most likely due to an attribute mapping problem with the Active Directory.</p> <ol style="list-style-type: none"> 1. Edit the particular Active Directory collector which is fetching the user's information from Active Directory. 2. Notice under optional attributes, there is a field name "Telephone Number" mapped to Active Directory attribute 'telephonenumber'. 4. Now, please use the Active Directory Explorer tool as described above to browse the Active Directory and see the correct attribute name. 3. Make sure that in Active Directory there is an attribute named 'telephonenumber' which has indeed the telephone number of the user. 5. Let us say in Active Directory it has been modified to 'phonenumber'. 6. Then Edit the CloudSecure User Directory collector. In optional attribute section, replace 'telephonenumber' with 'phonenumber'. 7. Save the Active Directory collector, the collector will restart and get the telephone number of the user and display the same in the user profile page.
<p>If encryption certificate (SSL) is enabled on the Active Directory (AD) Server, the Workload Security User Directory Collector can not connect to the AD Server.</p>	<p>Disable AD Server encryption before Configuring a User Directory Collector. Once the user detail is fetched it will be there for 13 months. If the AD server gets disconnected after fetching the user details, the newly added users in AD won't get fetched. To fetch again, the user directory collector needs to be connected to AD.</p>
<p>Data from Active Directory is present in CloudInsights Security. Want to delete all the user information from CloudInsights.</p>	<p>It is not possible to ONLY delete Active Directory user information from CloudInsights Security. In order to delete the user, the complete tenant needs to be deleted.</p>

Configuring an LDAP Directory Server Collector

You configure Workload Security to collect user attributes from LDAP Directory servers.

Before you begin

- You must be a Cloud Insights Administrator or Account Owner to perform this task.
- You must have the IP address of the server hosting the LDAP Directory server.

- An Agent must be configured before you configure an LDAP Directory connector.

Steps to Configure a User Directory Collector

- In the Workload Security menu, click:

Admin > Data Collectors > User Directory Collectors > + User Directory Collector and select **LDAP Directory Server**

The system displays the Add User Directory screen.

Configure the User Directory Collector by entering the required data in the following tables:

Name	Description
Name	Unique name for the user directory. For example <i>GlobalLDAPCollector</i>
Agent	Select a configured agent from the list
Server IP/Domain Name	IP address or Fully-Qualified Domain Name (FQDN) of server hosting the LDAP Directory Server
Search Base	<p>Search Base of the LDAP server Search Base allows both of the following formats:</p> <p><i>x.y.z</i> ⇒ direct domain name as you have it on your SVM. [Example: <i>hq.companyname.com</i>]</p> <p><i>DC=x,DC=y,DC=z</i> ⇒ Relative distinguished names [Example: <i>DC=hq,DC= companyname,DC=com</i>]</p> <p>Or you can specify as the following:</p> <p><i>OU=engineering,DC=hq,DC= companyname,DC=com</i> [to filter by specific OU engineering]</p> <p><i>CN=username,OU=engineering,DC=companyname,DC=netapp, DC=com</i> [to get only specific user with <username> from OU <engineering>]</p> <p><i>CN=Acrobat Users,CN=Users,DC=hq,DC=companyname,DC=com,O= companyname,L=Boston,S=MA,C=US</i> [to get all Acrobat Users within the Users in that organization]</p>
Bind DN	User permitted to search the directory. For example: <i>uid=ldapuser,cn=users,cn=accounts,dc=domain,dc= companyname,dc=com</i> <i>uid=john,cn=users,cn=accounts,dc=dorp,dc=company,dc=com</i> for a user john@dorp.company.com . <i>dorp.company.com</i>
--accounts	--users
--john	--anna

BIND password	Directory server password (i.e. password for username used in Bind DN)
Protocol	ldap, ldaps, ldap-start-tls
Ports	Select port

|While adding LDAP directory the following error is shown:

“Failed to determine the health of the collector within 2 retries, try restarting the collector again(Error Code: AGENT008)”

|Ensure correct Server IP and Search Base is provided

|Adding an LDAP Directory connector results in the ‘RETRYING’ state. Shows error “Unable to define state of the collector,reason Tcp command [Connect(localhost:35012,None,List(),Some(,seconds),true)] failed because of java.net.ConnectionException:Connection refused.”

|Incorrect IP or FQDN provided for the AD Server. Edit and provide the correct IP address or FQDN.

security login show -vserver svmname

Vserver: svmname

Authentication Acct Is-Nsswitch

User/Group Name Application Method Role Name Locked Group

vsadmin http password vsadmin yes no

vsadmin ontapi password vsadmin yes no

vsadmin ssh password vsadmin yes no

3 entries were displayed.

a. Install **selinux** (dependency package for the docker-ce):

```
wget http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-
selinux-2.68-1.el7.noarch.rpm
yum install -y container-selinux-2.68-1.el7.noarch.rpm
```

1. Install the docker-ce (not the native docker) package. You must use a version higher than 17.03:
https://download.docker.com/linux/centos/7/x86_64/stable/Packages/

2. SSH to the Redhat EC2 VM:

```
ssh -i "your_new_pem.pem" <ec2_hostname_or_IP>
sudo su -
```

3. Perform a docker login after installing the required AWS CLI package:

```

curl "https://s3.amazonaws.com/aws-cli/awscli-bundle.zip" -o "awscli-
bundle.zip"
unzip awscli-bundle.zip
sudo ./awscli-bundle/install -i /usr/local/aws -b /usr/local/bin/aws
/usr/local/bin/aws --version
aws configure --profile collector_READONLY
aws ecr get-login --no-include-email --region us-east-1 --profile
collector_READONLY
docker login -u AWS -p <token_generated_above> <ECR_hostname>

```

4. Use the following command to verify the steps completed successfully and the `cs-ontap-dsc` image can be successfully pulled:

```

docker pull 376015418222.dkr.ecr.us-east-1.amazonaws.com/cs-ontap-
dsc:1.25.0

```

Install the Workload Security Agent

1. Log in as Administrator or Account Owner to your Cloud Insights environment.
2. Navigate to Workload Security **Admin > Data Collectors** and click the **Agents** tab.
3. Click **+Agent** and specify RHEL as the target platform.
4. Copy the Agent Installation command.
5. Paste the Agent Installation command into the RHEL EC2 instance you are logged in to.
This installs the Workload Security agent, providing all of the [Agent Prerequisites](#) are met.

For detailed steps please refer to this xref:./

https://docs.netapp.com/us-en/cloudinsights/task_cs_add_agent.html#steps-to-install-agent

Troubleshooting

Known problems and their resolutions are described in the following table.

Problem	Resolution
<p>"Workload Security: Failed to determine ONTAP type for Amazon FSxN data collector" error is shown by the Data Collector.</p> <p>Customer is unable to add new Amazon FSxN data collector into Workload Security. Connection to FSxN cluster on port 443 from the agent is timing out. Firewall and AWS security groups have the required rules enabled to allow communication. An agent is already deployed and is in the same AWS account as well. This same agent is used to connect and monitor the remaining NetApp devices (and all of them are working).</p>	<p>Solve this issue by adding fsxadmin LIF network segment to agent's security rule. Allowed all ports if you are not sure about the ports.</p>

User Management

Workload Security user accounts are managed through Cloud Insights.

Cloud Insights provides four user account levels: Account Owner, Administrator, User, and Guest. Each account is assigned specific permission levels. A User account that has Administrator privileges can create or modify users, and assign each user one of the following Workload Security roles:

Role	Workload Security Access
Administrator	Can perform all Workload Security functions, including those for Alerts, Forensics, data collectors, automated response policies, and APIs for Workload Security. An Administrator can also invite other users but can only assign Workload Security roles.
User	Can view and manage Alerts and view Forensics. User role can change alert status, add a note, take snapshots manually, and restrict user access.
Guest	Can view Alerts and Forensics. Guest role cannot change alert status, add a note, take snapshots manually, or restrict user access.

Steps

1. Log into Workload Security
2. In the menu, click **Admin > User Management**

You will be forwarded to Cloud Insights's User Management page.

3. Select the desired role for each user.

While adding a new user, simply select the desired role (usually User or Guest).

More information on User accounts and roles can be found in the Cloud Insights [User Role](#) documentation.

SVM Event Rate Checker (Agent Sizing Guide)

The Event Rate Checker is used to check the NFS/SMB combined event rate in the SVM before installing an ONTAP SVM data collector, to see how many SVMs one Agent machine will be able to monitor. Use the Event Rate Checker as a sizing guide to help plan your security environment.

An Agent can support up to 50 data collectors.

Requirements:

- Cluster IP
- Cluster admin username and password



When running this script no ONTAP SVM Data Collector should be running for the SVM for which event rate is being determined.

Steps:

1. Install the Agent by following the instructions in CloudSecure.
2. Once the agent is installed, run the `server_data_rate_checker.sh` script as a sudo user:

```
/opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
```

3. This script requires `sshpass` to be installed in the linux machine. There are two ways to install it:

- a. Run the following command:

```
linux_prompt> yum install sshpass
```

- b. If that does not work, then download `sshpass` to the linux machine from the web and run the following command:

```
linux_prompt> rpm -i sshpass
```

4. Provide the correct values when prompted. See below for an example.
5. The script will take approximately 5 minutes to run.
6. After the run is complete, the script will print the event rate from the SVM. You can check Event rate per SVM in the console output:

```
"Svm svm_rate is generating 100 events/sec".
```

Each Ontap SVM Data Collector can be associated with a single SVM, which means each data collector will be able to receive the number of events which a single SVM generates.

Keep the following in mind:

A) Use this table as a general sizing guide:

Agent Machine Configuration	Number of SVM Data Collectors	Max event Rate which the Agent Machine can handle
4 core, 16GB	10 data collectors	20K events/sec
4 core, 32GB	20 data collectors	20K events/sec

B) To calculate your total events, add the Events generated for all SVMs for that agent.

C) If the script is not run during peak hours or if peak traffic is difficult to predict, then keep an event rate buffer of 30%.

B + C Should be less than A, otherwise the Agent machine will fail to monitor.

In other words, the number of data collectors which can be added to a single agent machine should comply to the formula below:

Sum of all Event rate of all Data Source Collectors + Buffer Event rate of 30% < 20000 events/second

See the [Agent Requirements](#) page for additional pre-requisites and requirements.

Example

Let us say we have three SVMs generating event rates of 100, 200, and 300 events per second, respectively.

We apply the formula:

(100+200+300) + [(100+200+300)*30%] = 600+180 = 780events/sec
780 events/second is < 20000 events/second, so the 3 SVMs can be monitored via one agent box.

Console output is available in the Agent machine in the file name *fpolicy_stat_<SVM Name>.log* in the present working directory.

The script may give erroneous results in the following cases:

- Incorrect credentials, IP, or SVM name are provided.
- An already-existing fpolicy with same name, sequence number, etc. will give error.
- The script is stopped abruptly while running.

An example script run is shown below:

```
[root@ci-cs-data agent]#  
/opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
```

```
Enter the cluster ip: 10.192.139.166
Enter the username to SSH: admin
Enter the password:
Getting event rate for NFS and SMB events.
Available SVMs in the Cluster
-----
QA_SVM
Stage_SVM
Qa-fas8020
Qa-fas8020-01
Qa-fas8020-02
audit_svm
svm_rate
vs_new
vs_new2
```

```
-----
Enter [1/5] SVM name to check (press enter to skip): svm_rate
Enter [2/5] SVM name to check (press enter to skip): audit_svm
Enter [3/5] SVM name to check (press enter to skip):
Enter [4/5] SVM name to check (press enter to skip):
Enter [5/5] SVM name to check (press enter to skip):
Running check for svm svm_rate...
Running check for svm audit_svm...
Waiting 5 minutes for stat collection
Stopping sample svm_rate_sample
Stopping sample audit_svm_sample
fpolicy stats of svm svm_rate is saved in fpolicy_stat_svm_rate.log
Svm svm_rate is generating 100 SMB events/sec and 100 NFS events/sec
Overall svm svm_rate is generating 200 events/sec
fpolicy stats of svm audit_svm is saved in fpolicy_stat_audit_svm.log
Svm audit_svm is generating 200 SMB events/sec and 100 NFS events/sec
Overall svm audit_svm is generating 300 events/sec
```

```
[root@ci-cs-data agent]#
```

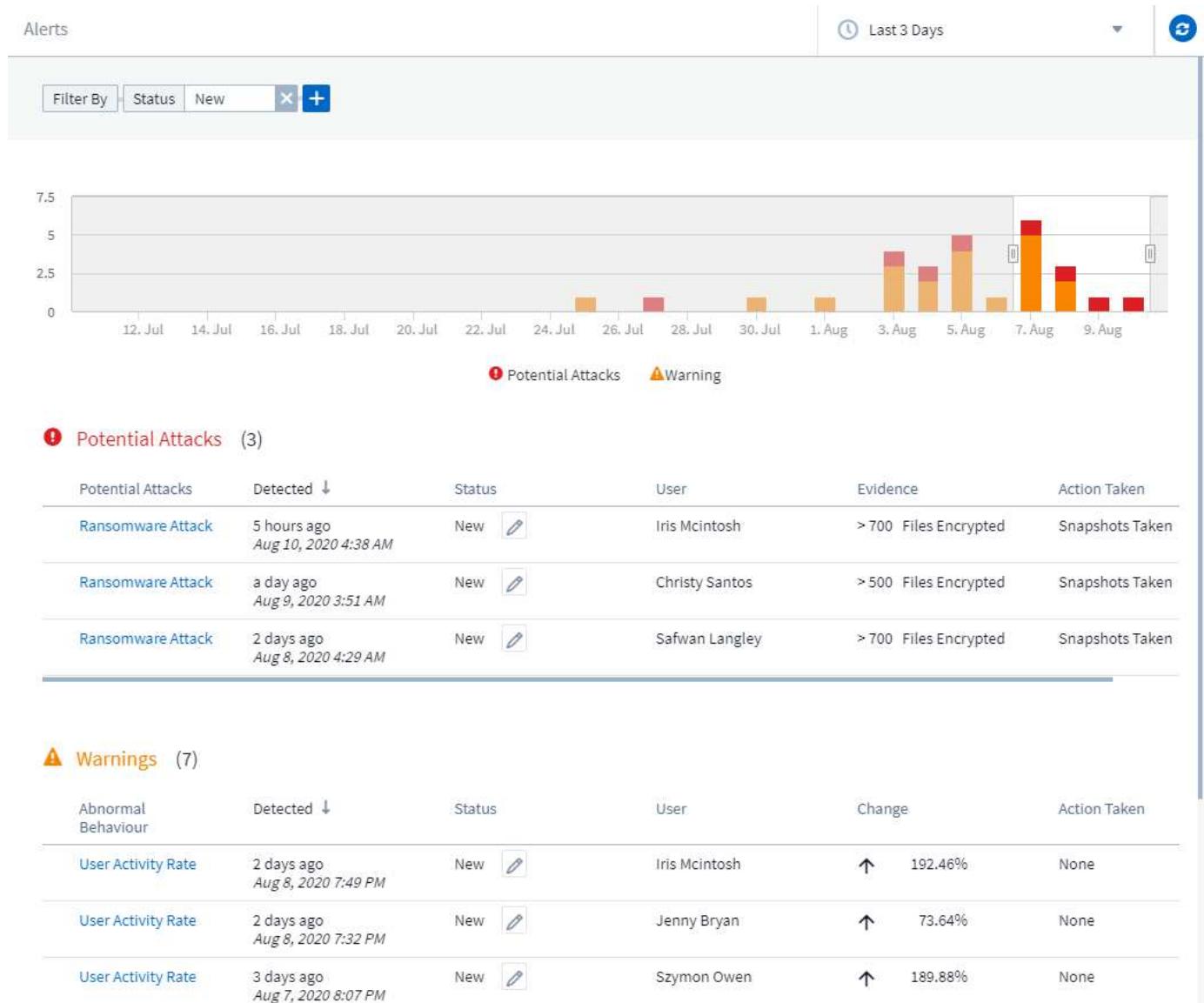
Troubleshooting

Question	Answer
----------	--------

If I run this script on an SVM that is already configured for Workload Security, does it just use the existing fpolicy config on the SVM or does it setup a temporary one and run the process?	The Event Rate Checker can run fine even for an SVM already configured for Workload Security. There should be no impact.
Can I increase the number of SVMs on which the script can be run?	Yes. Simply edit the script and change the max number of SVMs from 5 to any desirable number.
If I increase the number of SVMs, will it increase the time of running of the script?	No. The script will run for a max of 5 minutes, even if the number of SVMs is increased.
Can I increase the number of SVMs on which the script can be run?	Yes. You need to edit the script and change the max number of SVMs from 5 to any desirable number.
If I increase the number of SVMs, will it increase the time of running of the script?	No. The script will run for a max of 5mins, even if the number of SVMs are increased.
What happens if I run the Event Rate Checker with an existing agent?	Running the Event Rate Checker against an already-existing agent may cause an increase in latency on the SVM. This increase will be temporary in nature while the Event rate Checker is running.

Alerts

The Workload Security Alerts page shows a timeline of recent attacks and/or warnings and allows you to view details for each issue.



Alert

The Alert list displays a graph showing the total number of Potential Attacks and/or Warnings that have been raised in the selected time range, followed by a list of the attacks and/or warnings that occurred in that time range. You can change the time range by adjusting the start time and end time sliders in the graph.

The following is displayed for each alert:

Potential Attacks:

- The *Potential Attack* type (for example, Ransomware or Sabotage)
- The date and time the potential attack was *Detected*

- The *Status* of the alert:
 - **New:** This is the default for new alerts.
 - **In Progress:** The alert is under investigation by a team member or members.
 - **Resolved:** The alert has been marked as resolved by a team member.
 - **Dismissed:** The alert has been dismissed as false positive or expected behavior.

An administrator can change the status of the alert and add a note to assist with investigation.



- The *User* whose behavior triggered the alert
- *Evidence* of the attack (for example, a large number of files was encrypted)
- The *Action Taken* (for example, a snapshot was taken)

Warnings:

- The *Abnormal Behavior* that triggered the warning
- The date and time the behavior was *Detected*
- The *Status* of the alert (New, In progress, etc.)
- The *User* whose behavior triggered the alert
- A description of the *Change* (for example, an abnormal increase in file access)
- The *Action Taken*

Filter Options

You can filter Alerts by the following:

- The *Status* of the alert
- Specific text in the *Note*
- The type of *Attacks/Warnings*

- The User whose actions triggered the alert/warning

The Alert Details page

You can click an alert link on the Alerts list page to open a detail page for the alert. Alert details may vary according to the type of attack or alert. For example, a Ransomware Attack detail page may show the following information:

Summary section:

- Attack type (Ransomware, Sabotage) and Alert ID (assigned by Workload Security)
- Date and Time the attack was detected
- Action Taken (for example, an automatic snapshot was taken. Time of snapshot is shown immediately below the summary section))
- Status (New, In Progress, etc.)

Attack Results section:

- Counts of Affected Volumes and Files
- An accompanying summary of the detection
- A graph showing file activity during the attack

Related Users section:

This section shows details about the user involved in the potential attack, including a graph of Top Activity for the user.

Alerts page (this example shows a potential ransomware attack):



Detail page (this example shows a potential ransomware attack):



POTENTIAL ATTACK: AL_305
Ransomware Attack

Detected
5 days ago
Jul 11, 2020 4:02 AM

Action Taken
None

Status
New

Total Attack Results

1 Affected Volumes | 0 Deleted Files | 4173 Encrypted Files

4173 Files have been copied, deleted, and potentially encrypted by 1 user account.

This is potentially a sign of ransomware attack.
The extension "crypt" was added to each file.

Encrypted Files

Activity per minute



Related Users



Kristjan Egilsson
Accountant
Finance

4173
Encrypted Files

Detected
5 days ago
Jul 11, 2020 4:02 AM

Action Taken
None



Username
us035

Email
Egilsson@netapp.com

Phone
387224312607

Department
Finance

Manager
Lyndsey Maddox

[View Activity Detail](#)

Top Activity Types
Activity per minute
Last access location: 10.197.144.115

Write Read Metadata Others



Take a Snapshot Action

Workload Security protects your data by automatically taking a snapshot when malicious activity is detected, ensuring that your data is safely backed up.

You can define [automated response policies](#) that take a snapshot when ransomware attack or other abnormal user activity is detected.

You can also take a snapshot manually from the alert page.

Automatic Snapshot taken:

POTENTIAL ATTACK: AL_307
Ransomware Attack

Detected
4 days ago
Jul 26, 2020 3:38 AM

Action Taken
Snapshots Taken

Status
In Progress

Last snapshots taken by Amit Schwartz
Jul 30, 2020 2:54 PM

How To:
Restore Entities

Re-Take Snapshots

Total Attack Results

Affected Volumes	Deleted Files	Encrypted Files
1	0	5148

5148 Files have been copied, deleted, and potentially encrypted by 1 user account.

This is potentially a sign of ransomware attack.
The extension "crypt" was added to each file.

Encrypted Files
Activity per minute

Related Users

Ewen Hall
Developer Engineering

5148
Encrypted Files

Detectd
4 days ago
Jul 26, 2020 3:38 AM

Action Taken
Snapshots Taken

Manual Snapshot:

Cloud Insights

MONITOR & OPTIMIZE Alerts / *Nabilah Howell* had an abnormal change in activity rate

Jul 23, 2020 - Jul 26, 2020 1:44 AM - 1:44 AM

CLOUD SECURE **ALERTS** **FORENSICS** **ADMIN** **HELP**

Alert Detail

WARNING: AL_306
Nabilah Howell had an abnormal change in activity rate.

Detectd
5 days ago
Jul 25, 2020 1:44 PM

Action Taken
None

Status
New

Recommendation: Setup an Automated Response Policy
An Automated Response Policy will trigger measures to contain the damage automatically when a future attack is detected. Try it now.

Take Snapshots **How To:** Restore Entities

Nabilah Howell's Activity Rate Change

Typical	Alert
122.8 Activities Per Minute	210 Activities Per Minute

Activity Rate
Activity per 5 minutes

Minimize

Alert Notifications

Email notifications of alerts are sent to an alert recipient list for every action on the alert. To configure alert recipients, click on **Admin > Notifications** and enter an email addresses for each recipient.

Retention Policy

Alerts and Warnings are retained for 13 months. Alerts and Warnings older than 13 months will be deleted. If the Workload Security environment is deleted, all data associated with the environment is also deleted.

Troubleshooting

Problem:	Try This:
For snapshots taken by Workload Security (CS), is there a purging/archiving period for CS snapshots?	No. There is no purging/archiving period set for CS snapshots. The user needs to define purging policy for CS snapshots. Please refer to the ONTAP documentation on how to setup the policies.
There is a situation where, ONTAP takes hourly snapshots per day. Will Workload Security (CS) snapshots affect it? Will CS snapshot take the hourly snapshot place? Will the default hourly snapshot get stopped?	Workload Security snapshots will not affect the hourly snapshots. CS snapshots will not take the hourly snapshot space and that should continue as before. The default hourly snapshot will not get stopped.
What will happen if the maximum snapshot count is reached in ONTAP?	<p>If the maximum Snapshot count is reached, subsequent Snapshot taking will fail and Workload Security will show an error message noting that Snapshot is full.</p> <p>User needs to define Snapshot policies to delete the oldest snapshots, otherwise snapshots will not be taken.</p> <p>In ONTAP 9.3 and earlier, a volume can contain up to 255 Snapshot copies. In ONTAP 9.4 and later, a volume can contain up to 1023 Snapshot copies.</p> <p>See the ONTAP Documentation for information on setting Snapshot deletion policy.</p>
Workload Security is unable to take snapshots at all.	<p>Make sure that the role being used to create snapshots has proper rights assigned.</p> <p>Make sure <code>csrole</code> is created with proper access rights for taking snapshots:</p> <pre>security login role create -vserver <vservername> -role csrole -cmddirname "volume snapshot" -access all</pre>
Situations are failing for older alerts on SVMs which were removed from Workload Security and subsequently added back again. For new alerts which occur after SVM is added again, snapshots are taken.	This is a rare scenario. In the event you experience this, log in to ONTAP and take the snapshots manually for the older alerts.
In the <i>Alert Details</i> page, the message “Last attempt failed” error is seen below the <i>Take Snapshot</i> button. Hovering over the error displays “Invoke API command has timed out for the data collector with id”.	This can happen when a data collector is added to Workload Security via SVM Management IP, if the LIF of the SVM is in <i>disabled</i> state in ONTAP. Enable the particular LIF in ONTAP and trigger <i>Take Snapshot manually</i> from Workload Security. The Snapshot action will then succeed.

Forensics

Forensics - All Activity

The All Activity page helps you understand the actions performed on entities in the Workload Security environment.

Examining All Activity Data

Click **Forensics > Activity Forensics** and click the **All Activity** tab to access the All Activity page. This page provides an overview of activities in your environment, highlighting the following information:

- A graph showing *Activity History* (accessed per minute/per 5 minutes/per 10 minutes based on selected global time range)

You can zoom the graph by dragging out a rectangle in the graph. The entire page will be loaded to display the zoomed time range. When zoomed in, a button is displayed that lets the user zoom out.

- A chart of *Activity Types*. To obtain activity history data by activity type, click on corresponding x-axis label link.
- A chart of Activity on *Entity Types*. To obtain activity history data by entity type, click on corresponding x-axis label link.
- A list of the *All Activity* data

The **All Activity** table shows the following information. Note that not all of these columns are displayed by default. You can select columns to display by clicking on the "gear" icon .

- The **time** an entity was accessed including the year, month, day, and time of the last access.
- The **user** that accessed the entity with a link to the [User information](#).
- The **activity** the user performed. Supported types are:
 - **Change Group Ownership** - Group Ownership is of file or folder is changed. For more details about group ownership please see [this link](#).
 - **Change Owner** - Ownership of file or folder is changed to another user.
 - **Change Permission** - File or folder permission is changed.
 - **Create** - Create file or folder.
 - **Delete** - Delete file or folder. If a folder is deleted, *delete* events are obtained for all the files in that folder and subfolders.
 - **Read** - File is read.
 - **Read Metadata** - Only on enabling folder monitoring option. Will be generated on opening a folder on Windows or Running “ls” inside a folder in Linux.
 - **Rename** - Rename file or folder.
 - **Write** - Data is written to a file.
 - **Write Metadata** - File metadata is written, for example, permission changed.
 - **Other Change** - Any other event which are not described above. All unmapped events are mapped to

“Other Change” activity type. Applicable to files and folders.

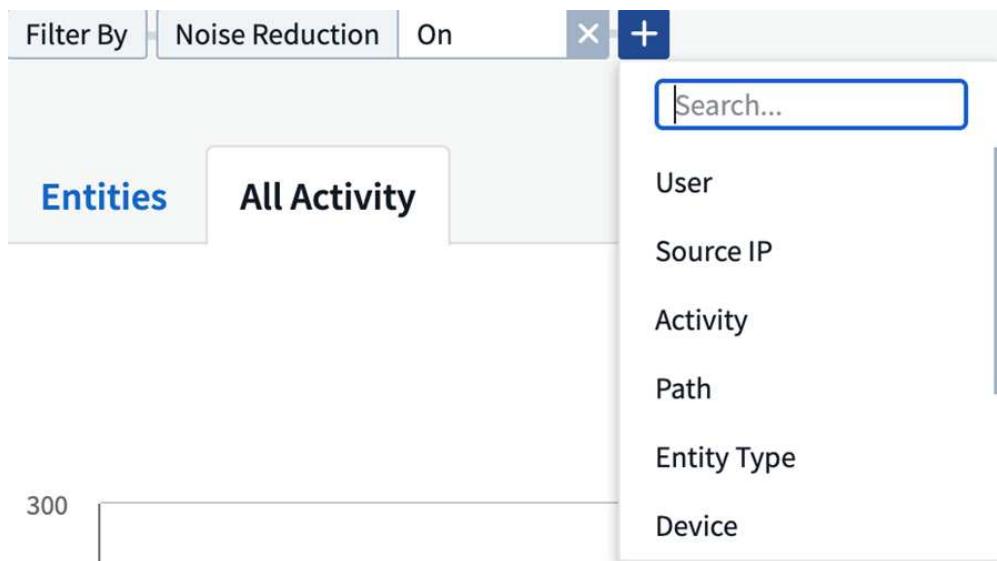
- The **Path** to the entity with a link to the [Entity Detail Data](#)
- The **Entity Type**, including entity (i.e. file) extension (.doc, .docx, .tmp, etc.)
- The **Device** where the entities reside
- The **Protocol** used to fetch events.
- The **Original Path** used for rename events when the original file was renamed. This column is not visible in the table by default. Use the column selector to add this column to the table.
- The **Volume** where the entities reside. This column is not visible in the table by default. Use the column selector to add this column to the table.

Filtering Forensic Activity History Data

There are two methods you can use to filter data.

1. Hover over the field in the table and click the filter icon that appears. The value is added to the appropriate filters in the top *Filter By* list.
2. Filter data by typing in the *Filter By* field:

Select the appropriate filter from the top ‘Filter By’ widget by clicking the **[+]** button:



Enter the search text

Press Enter or click outside of the filter box to apply the filter.

You can filter Forensic Activity data by the following fields:

- The **Activity** type.
- **Source IP** from which the entity was accessed. You must provide a valid source IP address in double quotes, for example “10.1.1.1”. Incomplete IPs such as “10.1.1.”, “10.1..*”, etc. will not work.
- **Protocol** to fetch protocol-specific activities.
- **Username** of the user performing the activity. You need to provide the exact Username to filter. Search

with partial username, or partial username prefixed or suffixed with '*' will not work.

- **Noise Reduction** to filter files which are created in the last 2 hours by the user. It is also used to filter temporary files (for example, .tmp files) accessed by the user.

The following fields are subject to special filtering rules:

- **Entity Type**, using entity (file) extension
- **Path** of the entity
- **User** performing the activity
- **Device** (SVM) where entities reside
- **Volume** where entities reside
- The **Original Path** used for rename events when the original file was renamed.

The preceding fields are subject to the following when filtering:

- Exact value should be within quotes: Example: "searchtext"
- Wildcard strings must contain no quotes: Example: searchtext, *searchtext*, will filter for any strings containing 'searchtext'.
- String with a prefix, Example: searchtext* , will search any strings which start with 'searchtext'.

Sorting Forensic Activity History Data

You can sort activity history data by *Time*, *User*, *Source IP*, *Activity*, *Path* and *Entity Type*. By default, the table is sorted by descending *Time* order, meaning the latest data will be displayed first. Sorting is disabled for *Device* and *Protocol* fields.

Exporting All Activity

You can export the activity history to a .CSV file by clicking the *Export* button above the Activity History table. Note that only the top 10,000 records are exported.

Column Selection for All Activity

The *All activity* table shows select columns by default. To add, remove, or change the columns, click the gear icon on the right of the table and select from the list of available columns.



Activity History Retention

Activity history is retained for 13 months for active Workload Security environments.

Applicability of Filters in Forensics Page

Filter	What it does	Example	Applicable in Which Filters?	Not applicable for which filters	Result

* (Asterisk)	enables you to search for everything	Auto*03172022	User, PATH, Entity Type, Device Type, Volume, Original Path		returns all resources that start with "Auto" and end with "03172022"
? (question mark)	enables you to search for a specific number of characters	AutoSabotageUser1_03172022?	User, Entity Type, Device, Volume		returns AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022AB, AutoSabotageUser1_031720225, and so on
OR	enables you to specify multiple entities	AutoSabotageUser1_03172022 OR AutoRansomUser4_03162022	User, Domain, Username, PATH, Entity Type, Device, Original Path		returns any of AutoSabotageUser1_03172022 OR AutoRansomUser4_03162022
NOT	allows you to exclude text from the search results	NOT AutoRansomUser4_03162022	User, Domain, Username, PATH, Entity Type, Original PATH, Volume	Device	returns everything that does not start with "AutoRansomUser4_03162022"
None	searches for NULL values in all fields	None	Domain		returns results where the target field is empty

Path / Original path Search

Search results with and without / will be different

/AutoDir1/AutoFile	Works
AutoDir1/AutoFile	Doesn't work
/AutoDir1/AutoFile (Dir1)	Dir1 Partial substring doesn't work
"/AutoDir1/AutoFile03242022"	Exact search works
Auto*03242022	Doesn't work
AutoSabotageUser1_03172022?	Doesn't work
/AutoDir1/AutoFile03242022 OR /AutoDir1/AutoFile03242022	Works
NOT /AutoDir1/AutoFile03242022	Works
NOT /AutoDir1	Works
NOT /AutoFile03242022	Doesn't work

*	Shows all the entries
---	-----------------------

Troubleshooting

Problem	Try This
In the “All Activities” table, under the ‘User’ column, the user name is shown as: “ldap:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817” or “ldap:default:80038003”	<p>Possible reasons could be:</p> <ol style="list-style-type: none"> 1. No User Directory Collectors have been configured yet. To add one, go to Admin > Data Collectors > User Directory Collectors and click on +User Directory Collector. Choose <i>Active Directory</i> or <i>LDAP Directory Server</i>. 2. A User Directory Collector has been configured, however it has stopped or is in error state. Please go to Admin > Data Collectors > User Directory Collectors and check the status. Refer to the User Directory Collector troubleshooting section of the documentation for troubleshooting tips. <p>After configuring properly, the name will get automatically resolved within 24 hours.</p> <p>If it still does not get resolved, check if you have added the correct User Data Collector. Make sure that the user is indeed part of the added Active Directory/LDAP Directory Server.</p>
Some NFS events are not seen in UI.	<p>Check the following:</p> <ol style="list-style-type: none"> 1. A user directory collector for AD server with POSIX attributes set should be running with the unixid attribute enabled from UI. 2. Any user doing NFS access should be seen when searched in the user page from UI 3. Raw events (Events for whom the user is not yet discovered) are not supported for NFS 4. Anonymous access to the NFS export will not be monitored. 5. Make sure NFS version used is lesser than NFS4.1.

Forensic Entities Page

The Forensics Entities page provides detailed information about entity activity in your environment.

Examining Entity Information

Click **Forensics > Activity Forensics** and click the *Entities* tab to access the Entities page.

This page provides an overview of entity activity in your environment, highlighting the following information:

- * A graph showing *Unique Entities* accessed per minute
- * A chart of *Entity Types Accessed*
- * A breakdown of the *Common Paths*
- * A list of the *Top 50 Entities* out of the total number of entities



Preview Top 50 Entities of 12386

Name	Entity Type	Device	Path	Activities ↓
Tech Tower.pptx	ppbx	demoGroupShares2	/ENG_CIFS_volume/Sales/Tech Tower.pptx	39
Kevin_Obrien.xlsx	xlsx	demoGroupShares2	/ENG_CIFS_volume/Sales/Kevin_Obrien.xlsx	37
Harrison_Ware.docx	docx	demoGroupShares2	/ENG_CIFS_volume/Sales/Harrison_Ware.docx	35
Matter Shop Lifters.pptx	ppbx	demoGroupShares2	/ENG_CIFS_volume/Sales/Matter_Shop_Lifters.pptx	35

Clicking on an entity in the list opens an overview page for the entity, showing a profile of the entity with details like name, type, device name, most accessed location IP, and path, as well as the entity behavior such as the user, IP, and time the entity was last accessed.

Forensics / Entities / Kevin_Obrien.xlsx



Entity Overview

Entity Profile		
Name Kevin_Obrien.xlsx	Most Accessed Location 10.197.144.115	Size 91 KB
Type xlsx	Device Name demoGroupShares2	Path /ENG_CIFS_volume/Sales/Kevin_Obrien.xlsx

Entity Behaviour	
Recent Activity	Operations (last 7 days)
Last accessed : 12 minutes ago Aug 24, 2020 2:02 PM	Read : 89
Last accessed by : Tyrique Ray	Read Metadata : 22
Last accessed from : 10.197.144.115	Other Activities : 43

Forensic User Overview

Information for each user is provided in the User Overview. Use these views to understand user characteristics, associated entities, and recent activities.

User Profile

User Profile information includes contact information and location of the user. The profile provides the following information:

- Name of the user
- Email address of the user
- User's Manager
- Phone contact for the user
- Location of the user

User Behavior

The user behavior information identifies recent activities and operations performed by the user. This information includes:

- Recent activity
 - Last access location
 - Activity graph
 - Alerts
- Operations for the last seven days
 - Number of operations

Refresh Interval

The User list is refreshed every 12 hours.

Retention Policy

If not refreshed again, the User list is retained for 13 months. After 13 months, the data will be deleted. If your Workload Security environment is deleted, all data associated with the environment is deleted.

Automated Response Policies

Response Policies trigger actions such as taking a snapshot or restricting user access in the event of an attack or abnormal user behavior.

You can set policies on specific devices or all devices. To set a response policy, select **Admin > Automated Response Policies** and click the appropriate *Policy button. You can create policies for Attacks or for Warnings.

Add Attack Policy X

Policy Name*
Unique New Policy Name

For Ransomware Attacks
Currently Cloud Secure discovers and tracks possible Ransomware attacks.
Coming Soon: Tracking for additional attack types, including Identity Theft, Sabotage, and Snooping.

On Device
All Devices ▼

+ Another Device

Actions
 Take Snapshot !

Cancel Save

You must save the policy with a unique name.

To disable an automated response action (for example, Take Snapshot), simply un-check the action and save the policy.

When an alert is triggered against the specified devices (or all devices, if selected), the automated response policy takes a snapshot of your data. You can see snapshot status on the [Alert detail page](#).

See the [Restrict User Access](#) page for more details on restricting user access by IP.

You can modify or pause an Automated Response Policy by choosing the option in the policy's drop-down menu.

Workload Security will automatically delete snapshots once per day based on the Snapshot Purge settings.

Snapshot Purge Settings



Define purge periods to automatically delete snapshots taken by Cloud Secure.

Attack Automated Response

Delete Snapshot after

Warning Automated Response

Delete Snapshot after

User Created

Delete Snapshot after

Integration with ONTAP Autonomous Ransomware Protection

The ONTAP Autonomous Ransomware Protection (ARP) feature uses workload analysis in NAS (NFS and SMB) environments to proactively detect and warn about abnormal in-file activity that might indicate a ransomware attack.

Additional details and license requirements about ARP can be found [here](#).

Workload Security integrates with ONTAP to receive ARP events and provide an additional analytics and automatic responses layer.

Workload Security receives the ARP events from ONTAP and takes the following actions:

1. Correlates volume encryption events with user activity to identify who is causing the damage.
2. Implements automatic response policies (if defined)
3. Provides forensics capabilities:
 - Allow customers to conduct data breach investigations.
 - Identify what files were affected, helping to recover faster and conduct data breach investigations.

Prerequisites

1. Minimum ONTAP version: 9.11.1
2. ARP enabled volumes. Details on enabling ARP can be found [here](#). ARP must be enabled via OnCommand System Manager. Workload Security cannot enable ARP.
3. Workload Security collector should be added via cluster IP.
4. Cluster level credentials are needed for this feature to work. In other words, cluster level credentials must be used when adding the SVM.

User permissions required

If you are using cluster administration credentials, no new permissions are needed.

If you are using a custom user (for example, *csuser*) with permissions given to the user, then follow the steps below to give permissions to Workload Security to collect ARP related information from ONTAP.

For *csuser* with cluster credentials, do the following from the ONTAP command line:

```
security login rest-role create -role arwrole -api /api/storage/volumes  
-access readonly -vserver <cluster_name>  
security login rest-role create -api /api/security/anti-ransomware -access  
readonly -role arwrole -vserver <cluster_name>  
security login create -user-or-group-name csuser -application http  
-authmethod password -role arwrole
```

Sample Alert

A sample alert generated due to ARP event is shown below:

POTENTIAL ATTACK: AL_1315
Ransomware Attack

Detected
5 months ago
Oct 20, 2022 3:06 AM

Action Taken
⚠ Access Blocked on 5 SVMs ⓘ
Snapshots Taken

Status
New

Last snapshots taken by auto response policy Oct 20, 2022 3:09 AM

How To: [Restore Entities](#)

[Change Block Period](#) [Re-Take Snapshots](#) [Unblock User](#)

Total Attack Results

1	Affected Volumes
83	Deleted Files
81	Encrypted Files

81 Files have been copied, deleted, and potentially encrypted by 1 user account.

The extension "osiris" was added to each file.

ⓘ High Confidence Detection
Ransomware behavior and in-file encryption activities were detected.

Encrypted Files
Activity per minute

Activity per minute

0 25 50

02:30 03:00 03:30 04:00 04:30 05:00

E Encryption activity in files

Related Users

Jamelia Graham Business Partner HR	User/IP Access ⓘ Blocked	81 Encrypted Files Detected 5 months ago Oct 20, 2022 3:06 AM
---	-----------------------------	---

Username us024
Domain cslab.netapp.com
Email Graham@netapp.com
Phone 9251140014

Department HR
Manager Iwan Holt
Location WA

Top Activity Types
Activity per minute
Last accessed from: 10.193.113.247

Activity per minute

0 50 100 150

02:30 03:00 03:30 04:00 04:30 05:00

Create Read Others

[View Activity Detail](#)

Access Limitation History for This User (3)

Time	Action	Duration	Action Taken by	Response	Blocked IPs on NFS
Oct 20, 2022 3:09 AM	⚠ Block more detail	Never Expires		Automatic	none
Mar 10, 2022 4:59 AM	Unblock		system	Blocking Expired	10.197.144.115
Mar 10, 2022 3:57 AM	⚠ Block more detail	1h		Automatic	10.197.144.115

Affected Devices/Volumes

Device ↑	Volume	Encrypted Files	Associated Snapshot Taken	
subprod_rtp	stargazer	81	Oct 20, 2022 3:09 AM	cloudsecure_attack_auto Automatic Take Snapshot

A high confidence banner indicates the attack has shown ransomware behavior along with file encryption

activities.

The encrypted files graph indicates the timestamp at which the volume encryption activity was detected by the ARP solution.

Limitations

In the case where an SVM is not monitored by Workload Security, but there are ARP events generated by ONTAP, the events will still be received and displayed by Workload Security. However, Forensic information related to the alert, as well as user mapping, will not be captured or shown.

Troubleshooting

Known problems and their resolutions are described in the following table.

Problem:	Resolution:
Email alerts are received 24 hrs after an attack is detected. In the UI, the alerts are shown 24 hrs before that when the emails are received by Cloud Insights Workload Security.	When ONTAP sends the <i>Ransomware Detected</i> Event to Cloud Insights Workload Security (i.e. Workload Security), the email is sent. The Event contains a list of attacks and its timestamps. The Workload Security UI displays the alert timestamp of the first file attacked. ONTAP sends the <i>Ransomware Detected</i> Event to Cloud Insights when a certain number of files are encoded. Therefore, there may be a difference between the time the alert is displayed in the UI and the time the email is sent.

Blocking User Access

Once an attack is detected, Workload Security can stop the attack by blocking user access to the file system. Access can be blocked automatically, using Automated Response Policies or manually from the alert or user details pages.

When blocking user access, you should define a blocking time period. After the selected time period ends, user access is automatically restored.

Access blocking is supported for both SMB and NFS protocols.

User is directly blocked for SMB and IP address of the host machines causing the attack will be blocked for NFS. Those machine IP addresses will be blocked from accessing any of the Storage Virtual Machines (SVMs) monitored by Workload Security.

For example, let's say Workload Security manages 10 SVMs and the Automatic Response Policy is configured for four of those SVMs. If the attack originates in one of the four SVMs, the user's access will be blocked in all 10 SVMs. A Snapshot is still taken on the originating SVM.

If there are four SVMs with one SVM configured for SMB, one configured for NFS, and the remaining two configured for both NFS and SMB, all the SVMs will be blocked if the attack originates in any of the four SVMs.

Prerequisites for User Access Blocking

Cluster level credentials are needed for this feature to work.

If you are using cluster administration credentials, no new permissions are needed.

If you are using a custom user (for example, *csuser*) with permissions given to the user, then follow the steps below to give permissions to Workload Security to block user.

For *csuser* with cluster credentials, do the following from the ONTAP command line:

```
security login role create -role csrole -cmddirname "vserver export-policy rule" -access all
security login role create -role csrole -cmddirname set -access all
security login role create -role csrole -cmddirname "vserver cifs session" -access all
security login role create -role csrole -cmddirname "vserver services access-check authentication translate" -access all
security login role create -role csrole -cmddirname "vserver name-mapping" -access all
```

How to enable the feature?

- In Workload Security, navigate to **Admin > Automated Response Policies > Response Policy Settings > Block User Access**.
- Set “Enable Block User Access” to *enabled*.

How to set up Automatic user access blocking?

- Create a new Attack Policy or edit an existing Attack policy.
- Select the SVMs on which the attack policy should be monitored.
- Click on the checkbox “Block User File Access”. The feature will be enabled when this is selected.
- Under “Time Period” select the time until which the blocking should be applied.
- To test automatic user blocking,, you can simulate an attack via a [simulated script](#).

How to know if there are blocked users in the system?

- In the alert lists page, a banner on the top of screen will be displayed in case any user is blocked.
- Clicking on the banner will take you to the “Users” page, where the list of blocked users can be seen.
- In the “Users” page, there in a column named “User/IP Access”. In that column, the current state of user blocking will be displayed.

Restrict and manage user access manually

- You can go to the alert details or user details screen and then manually block or restore a user from those screens.

User Access Limitation History

In the alert details and user details page, in the user panel, you can view an audit of the user’s access limitation history: Time, Action (Block, Unblock), duration, action taken by, manual/automatic, and affected IPs for NFS.

How to disable the feature?

At any time, you can disable the feature. If there are restricted users in the system, you must restore their access first.

- In Workload Security, navigate to **Admin > Automated Response Policies > Response Policy Settings > Block User Access**
- De-select “Enable Block User Access” to disable.

The feature will be hidden from all pages.

Manually Restore IPs for NFS

Use the following steps to manually restore any IPs from ONTAP if your Workload Security trial expires, or if the agent/collector is down.

1. List all export policies on an SVM.

```
contrail-qa-fas8020::> export-policy rule show -vserver <svm name>
      Policy          Rule   Access     Client           RO
Vserver    Name        Index  Protocol Match       Rule
-----
-----
svm0      default      1      nfs3,      cloudsecure_rule, never
                  nfs4,      10.11.12.13
                  cifs
svm1      default      4      cifs,      0.0.0.0/0      any
                  nfs
svm2      test         1      nfs3,      cloudsecure_rule, never
                  nfs4,      10.11.12.13
                  cifs
svm3      test         3      cifs,      0.0.0.0/0      any
                  nfs,
                  flexcache
4 entries were displayed.
```

2. Delete the rules across all policies on the SVM which have “cloudsecure_rule” as Client Match by specifying its respective RuleIndex. Workload Security rule will usually be at 1.

```
contrail-qa-fas8020::*> export-policy rule delete -vserver <svm name>
-policyname * -ruleindex 1
```

3. Ensure Workload Security rule is deleted (optional step to confirm).

```
contrail-qa-fas8020::*> export-policy rule show -vserver <svm name>
      Policy          Rule   Access     Client           RO
Vserver    Name        Index  Protocol Match       Rule
-----
-----
svm0      default      4      cifs,      0.0.0.0/0      any
                  nfs
svm2      test         3      cifs,      0.0.0.0/0      any
                  nfs,
                  flexcache
2 entries were displayed.
```

Manually Restore Users for SMB

Use the following steps to manually restore any users from ONTAP if your Workload Security trial expires, or if the agent/collector is down.

You can get the list of users blocked in Workload Security from the users list page.

1. Login to the ONTAP cluster (where you want to unblock users) with cluster *admin* credentials. (For Amazon FSx, login with FSx credentials).
2. Run the following command to list all users blocked by Workload Security for SMB in all SVMs:

```
vserver name-mapping show -direction win-unix -replacement " "
```

```
Vserver: <vservername>
Direction: win-unix
Position Hostname IP Address/Mask
-----
1      -          -          Pattern: CSLAB\\US040
                           Replacement:
2      -          -          Pattern: CSLAB\\US030
                           Replacement:
2 entries were displayed.
```

In the above output, 2 users were blocked (US030, US040) with domain CSLAB.

1. Once we identify the position from the above output, run the following command to unblock the user:

```
vserver name-mapping delete -direction win-unix -position <position>
```

2. Confirm the users are unblocked by running the command:

```
vserver name-mapping show -direction win-unix -replacement " "
```

No entries should be displayed for the users previously blocked.

Troubleshooting

Problem	Try This
Some of the users are not getting restricted, though there is an attack.	<p>1. Make sure that the Data Collector and Agent for the SVMs are in <i>Running</i> state. Workload Security won't be able to send commands if the Data Collector and Agent are stopped.</p> <p>2. This is because the user may have accessed the storage from a machine with a new IP which has not been used before. Restricting happens via IP address of the host through which the user is accessing the storage. Check in the UI (Alert Details > Access Limitation History for This User > Affected IPs) for the list of IP addresses which are restricted. If the user is accessing storage from a host which has an IP different from the restricted IPs, then the user will still be able to access the storage through the non-restricted IP. If the user is trying to access from the hosts whose IPs are restricted, then the storage won't be accessible.</p>
Manually clicking on Restrict Access gives "IP addresses of this user have already been restricted".	The IP to be restricted is already being restricted from another user.
Policy could not be modified. Reason: not authorized for that command.	Check if using csuser, permissions are given to the user as mentioned above.
User (IP Address) blocking for NFS works, but for SMB / CIFS, I see an error message: "SID to DomainName transformation failed. Reason timeout: socket is not established"	<p>This can happen if <i>csuser</i> does not have permission to perform ssh. (Ensure connection at cluster level, then ensure user can perform ssh). <i>csuser</i> role requires these permissions.</p> <p>https://docs.netapp.com/us-en/cloudinsights/cs_restrict_user_access.html#prerequisites-for-user-access-blocking</p> <p>For <i>csuser</i> with cluster credentials, do the following from the ONTAP command line:</p> <pre>security login role create -role csrole -cmddirname "vserver export-policy rule" -access all security login role create -role csrole -cmddirname set -access all security login role create -role csrole -cmddirname "vserver cifs session" -access all security login role create -role csrole -cmddirname "vserver services access-check authentication translate" -access all security login role create -role csrole -cmddirname "vserver name-mapping" -access all</pre> <p>If <i>csuser</i> is not used and if admin user at cluster level is used, make sure that the admin user has ssh permission to ONTAP.</p>

Workload Security: Simulating an Attack

You can use the instructions on this page to simulate an attack for testing or demonstrating Workload Security using the included Ransomware Simulation script.

Things to note before you begin

- The ransomware simulation script works on Linux only.
- The script is provided with the Workload Security agent installation files. It is available on any machine that has a Workload Security agent installed.
- You can run the script on the Workload Security agent machine itself; there is no need to prepare another Linux machine. However, if you prefer to run the script on another system, simply copy the script and run it there.

Have at least 1,000 sample files

This script should run on an SVM with a folder that has files to encrypt. We recommend having at least 1,000 files within that folder and any sub-folders. The files must not be empty.

Do not create the files and encrypt them using the same user. Workload Security considers this a low-risk activity and will therefore not generate an alert (i.e. the same user modifies files he/she/they just created).

See below for instructions to [programmatically create non-empty files](#).

Guidelines before you run the simulator:

1. Make sure encrypted files are not empty.
2. Make sure you encrypt > 50 files. A small number of files will be ignored.
3. Do not run an attack with the same user multiple times. After a few times, CS will learn this user behavior and assume it is the user's normal behavior.
4. Do not encrypt files the same user has just created. Changing a file that was just created by a user is not considered a risky activity. Instead, use files created by another user OR wait for a few hours between creating the files and encrypting them.

Prepare the system

First, mount the target volume to machine. You can mount either an NFS mount or CIFs export.

To mount NFS export in Linux:

```
mount -t nfs -o vers=4.0 10.193.177.158:/svmvol1 /mntpt  
mount -t nfs -o vers=4.0 Vserver data IP>:/nfsvol /destinationlinuxfolder
```

Do not mount NFS version 4.1; it is not supported by Fpolicy.

To mount CIFs in Linux:

```
mount -t cifs //10.193.77.91/sharedfolderincluster  
/root/destinationfolder/ -o username=raisa
```

Next, set up a Data Collector:

1. Configure the Workload Security agent if not already done.
2. Configure SVM data collector if not already done.

Run the Ransomware Simulator script

1. Log in (ssh) to the Workload Security agent machine.
2. Navigate to: */opt/netapp/cloudsecure/agent/install*
3. Call the simulator script without parameters to see usage:

```
# pwd  
/opt/netapp/cloudsecure/agent/install  
# ./ransomware_simulator.sh  
Error: Invalid directory provided.  
Usage: ./ransomware_simulator.sh [-e] [-d] [-i <input_directory>]  
      -e to encrypt files (default)  
      -d to restore files  
      -i <input_directory> - Files under the directory to be encrypted
```

```
Encrypt command example: ./ransomware_simulator.sh -e -i  
/mnt/audit/reports/  
Decrypt command example: ./ransomware_simulator.sh -d -i  
/mnt/audit/reports/
```

Encrypt your test files

To encrypt the files, run the following command:

```
# ./ransomware_simulator.sh -e -i /root/for/  
Encryption key is saved in /opt/netapp/cloudsecure/cloudsecure-agent-  
1.251.0/install/encryption-key,  
which can be used for restoring the files.  
Encrypted /root/for/File000.txt  
Encrypted /root/for/File001.txt  
Encrypted /root/for/File002.txt  
...
```

Restore files

To decrypt, run the following command:

```
[root@scspa2527575001 install]# ./ransomware_simulator.sh -d -i /root/for/
File /root/for/File000.txt is restored.
File /root/for/File001.txt is restored.
File /root/for/File002.txt is restored.
...
```

Run the script multiple times

After generating a ransomware attack for a user, switch to another user in order to generate an additional attack.

Workload Security learns user behavior and will not alert on repeated ransomware attacks within a short duration for the same user.

Create files programmatically

Before creating the files, you must first stop the data collector processing.

Perform the steps below before you add the data collector to the Agent. If you have already added the data collector, just edit the data collector, enter an invalid password, and save it. This will temporarily put the data collector in error state. NOTE: Be sure you note the original password!

Before running the simulation, you must first add files to be encrypted. You can either manually copy the files to be encrypted into the target folder, or use a script (see the example below) to programmatically create the files. Whichever method you use, copy at least 1,000 files.

If you choose to programmatically create the files, do the following:

1. Log into the Agent box.
2. Mount an NFS export from the SVM of the filer to the Agent machine. Cd to that folder.
3. In that folder create a file named createfiles.sh
4. Copy the following lines to that file.

```
for i in {000..1000}
do
    echo hello > "File${i}.txt"
done
echo 3 > /proc/sys/vm/drop_caches ; sync
```

5. Save the file.
6. Ensure execute permission on the file:

```
chmod 777 ./createfiles.sh
```

7. Execute the script:

```
./createfiles.sh
```

1000 files will be created in the current folder.

8. Re-enable the data collector

If you disabled the data collector in step 1, edit the data collector, enter the correct password, and save. Make sure that the data collector is back in running state.

Configuring Email Notifications for Alerts, Warnings, and Agent/Data Source Collector health

To configure Workload Security alert recipients, click on **Admin > Notifications** and enter an email addresses in the appropriate section(s) for each recipient.

Potential Attack Alerts and Warnings

To send *Potential Attack* alert notifications, enter the recipients' email addresses in the *Send Potential Attack Alerts* section.

Email notifications are sent to the alert recipient list for every action on the alert.

To send *Warning* notifications, enter the recipients' email addresses in the *Send Warning Alerts* section.

Agent and Data Collector Health monitoring

You can monitor the health of Agents and Data Sources through notifications.

In order to receive notifications in the event that an Agent or Data Source collector is not functioning, enter the email addresses of the recipients in the *Data Collection Health Alerts* section.

Keep the following in mind:

- Health alerts will be sent only after the agent/collector stops reporting for at least one hour.
- Only one email notification is sent to the intended recipients in a given 24 hour period, even if the Agent or Data collector is disconnected for a longer duration.
- In case of an Agent failure, one alert will be sent (not one per collector). The email will include a list of all impacted SVMs.
- Active directory collection failure is reported as a warning; it does not impact Ransomware detection.
- The Getting Started setup list now includes a new *Configure email notifications* phase.

Workload Security API

The Workload Security API enables NetApp customers and independent software vendors (ISVs) to integrate Workload Security with other applications, such as CMDB's or other ticketing systems.

Requirements for API Access:

- An API Access Token model is used to grant access.
- API Token management is performed by Workload Security users with the Administrator role.

API Documentation (Swagger)

The latest API information is found by logging in to Workload Security and navigating to **Admin > API Access**. Click the **API Documentation** link.

The API Documentation is Swagger-based, which provides a brief description and usage information for the API and allows you to try it out in your environment.

API Access Tokens

Before using the Workload Security API, you must create one or more **API Access Tokens**. Access tokens grant read permissions. You can also set the expiration for each access token.

To create an Access Token:

- Click **Admin > API Access**
- Click **+API Access Token**
- Enter **Token Name**
- Specify **Token Expiration**

 Your token will only be available for copying to the clipboard and saving during the creation process. Tokens can not be retrieved after they are created, so it is highly recommended to copy the token and save it in a secure location. You will be prompted to click the Copy API Access Token button before you can close the token creation screen.

You can disable, enable, and revoke tokens. Tokens that are disabled can be enabled.

Tokens grant general purpose access to APIs from a customer perspective, managing access to APIs in the scope of their own environment.

The application receives an Access Token after a user successfully authenticates and authorizes access, then passes the Access Token as a credential when it calls the target API. The passed token informs the API that the bearer of the token has been authorized to access the API and perform specific actions based on the scope that was granted during authorization.

The HTTP header where the Access Token is passed is **X-CloudInsights-ApiKey**:

For example, use the following to retrieve storage assets:

```
curl https://<tenant_host_name>/rest/v1/cloudsecure/activities -H 'X-CloudInsights-ApiKey: <API_Access_Token>'
```

Where *<API_Access_Token>* is the token you saved during API access key creation.

Detailed information can be found in the *API Documentation* link under **Admin > API Access**.

Active IQ

NetApp **Active IQ** provides a series of visualizations, analytics, and other support-related services to NetApp customers for their hardware / software systems. The data reported by Active IQ can enhance troubleshooting of system problems and also provide insight into optimization and predictive analysis related to your devices.

Cloud Insights collects the **Risks** for any NetApp Clustered Data ONTAP storage system that is monitored and reported by Active IQ. Risks reported for the storage systems are collected automatically by Cloud Insights as part of its data collection from those devices. You must add the appropriate data collector to Cloud Insights to collect Active IQ risk information.

Cloud Insights will not show risk data for ONTAP systems that are not monitored and reported by Active IQ.

The risks reported are shown in Cloud Insights on the *storage* and *storage node* asset landing pages, in the "Risks" table. The table shows Risk Detail, Category of risk, and Potential Impact of the risk, and also provides a link to the Active IQ page summarizing all risks for the storage node (NetApp Support account sign-in required).

Risks				
108 items found				
Object ↑	Risk Detail	Category	Potential Impact	Source
 tawny01	The following certificates have expired or are expiring within 30 days: Expired: 53CF9553, 53C504D4, 53D671B4, Expiring within 30 days: None	System Configuration	Clients may not be able to connect to the cluster over secure (SSL based) protocols.	
 tawny01	None of the NIS servers configured for SVM(s) tawny_svm_oc_markc can be contacted.	CIFS Protocol	Potential CIFS and NFS outages may occur.	
 tawny01	ONTAP version 8.3.2 has entered the Self-Service Support period.	ONTAP	Self-Service Support is the time period where NetApp does not provide support for a version of a software product, but related documentation is still available on the NetApp Support Site.	

A count of reported risks is also shown in the landing page's Summary widget, with a link to the appropriate Active IQ page. On a *storage* landing page, the count is a sum of risks from all underlying storage nodes.

Storage Summary			
Model: FAS6210	Microcode Version: 8.3.2 clustered Data ONTAP	Management: HTTPS://10.197.143.25:443	
Vendor: NetApp	Raw Capacity: 80,024.3 GB	FC Fabrics Connected: 0	
Family: FAS6200	Latency - Total: 0.77 ms	Performance Policies:	
Serial Number: 1-80-000013	IOPS - Total: 1,819.19 IO/s	Risks:	 108 risks detected by 
IP: 10.197.143.25	Throughput - Total: 41.69 MB/s		

Opening the Active IQ page

When clicking on the link to an Active IQ page, if you are not currently signed in to your Active IQ account, you must perform the following steps to view the Active IQ page for the storage node.

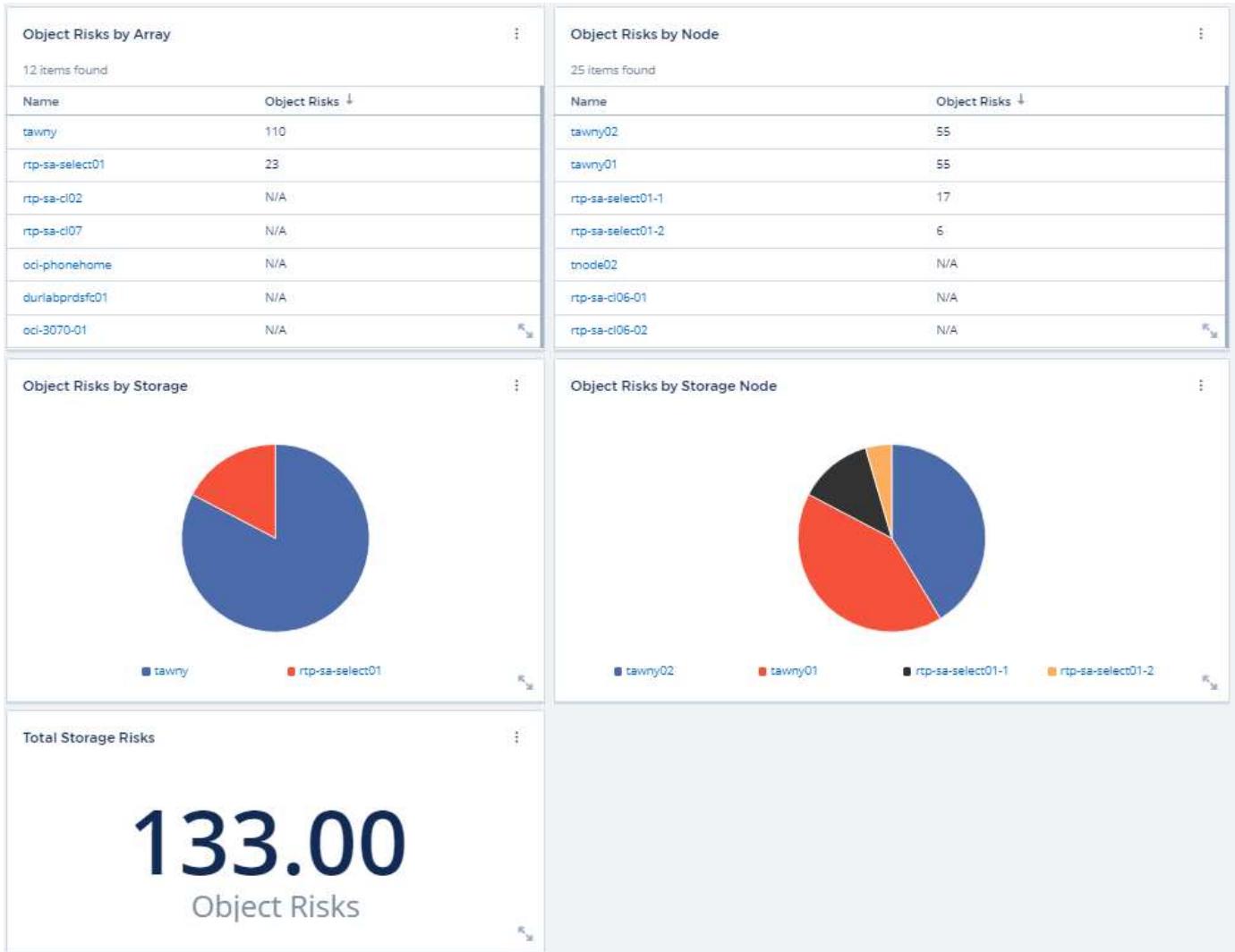
1. In the Cloud Insights Summary widget or Risks table, click the "Active IQ" link.
2. Sign in to your NetApp Support account. You are taken directly to the storage node page in Active IQ.

Querying for Risks

In Cloud Insights, you can add the **monitoring.count** column to a storage or storage node query. If the returned result includes Active IQ-Monitored storage systems, the monitoring.count column will display the number of risks for the storage system or node.

Dashboards

You can build widgets (e.g. pie chart, table widget, bar, column, scatter plot, and single value widgets) in order to visualize object risks for storage and storage nodes for NetApp Clustered Data ONTAP systems monitored by Active IQ. "Object Risks" can be selected as a column or metric in these widgets where Storage or Storage Node is the object of focus.



Troubleshooting

Troubleshooting General Cloud Insights Problems

Here you will find suggestions for troubleshooting Cloud insights.

See also [Troubleshooting Linux Acquisition Unit Problems](#) and [Troubleshooting Windows Acquisition Unit Problems](#).

Login issues:

Problem:	Try this:
Cloud Insights logs out every 5 minutes	<p>Enable third-party acceptance for the necessary NetApp and auth0 cookies.</p> <p>Example: In Chrome, enter "chrome://settings/cookies" in the browser URL.</p> <p>Select the "Allow all cookies" option. OR Select "Block third-party cookies" and add exceptions for [.]auth0.com and [.]netapp.com.</p> <p>Note: Make sure to select the "Including third-party cookies on this site" option when creating an exception.</p>
I have a Cloud Central account but am unable to login to Cloud Central.	<p>Open a ticket from https://mysupport.netapp.com/site/help. Select category "cloud.netapp.com > Account/Login issues" or "cloud.netapp.com > Federation issues". This is specifically for Cloud Central issues or questions.</p> <p>For all other Cloud Insights technical support issues, contact NetApp support.</p>
I got invited to Cloud Insights but I get a "not authorized" message.	<p>Verify that you have signed up for a Cloud Central account, or that your organization uses SSO login with Cloud Central.</p> <p>Verify your Cloud Central profile email address matches email address shown in your Cloud Insights welcome email. If the email does not match, request a new invitation with the correct email address.</p>
I logged out from Cloud Central or Cloud Secure and was automatically logged out from Cloud Insights.	Single Sign-On (SSO) across NetApp Cloud logs out all Cloud Insights, Cloud Secure, and Reporting sessions. If you have access to multiple Cloud Insights accounts, logging out from any one logs out all active sessions. Log back in to access your account.

Problem:	Try this:
I was automatically logged out after several days.	NetApp Cloud accounts require reauthentication every few days (current Cloud Central setting is 7 days). Log back in to access your account.
I receive an error message “no longer authorized to login”.	Contact your account administrator to verify access to Cloud Insights. Verify your Cloud Central profile email address matches email address shown in your Cloud Insights welcome email
Other login errors	Try incognito mode in Chrome, or clear browser history, cookies, and cache. Try with a different browser profile (i.e. Chrome - add Person).

If you have an active Cloud Insights subscription you can use these support options:

[Phone](#)

[Support Ticket](#)

For more information, see the [Cloud Insights Support Documentation](#).

Troubleshooting Acquisition Unit Problems on Linux

Here you will find suggestions for troubleshooting problems with Acquisition Units on a Linux server.

Problem:	Try this:
AU status on the Admin > Data Collectors page in the Acquisition Units tab displays "Certificate Expired" or "Certificate Revoked".	<p>Click on the menu to the right of the AU and select Restore Connection. Follow the instructions to restore your Acquisition Unit:</p> <ol style="list-style-type: none">1. Stop the Acquisition Unit (AU) service. You can click the <i>Copy Stop Command</i> button to quickly copy the command to the clipboard, then paste this command into a command prompt on the acquisition unit machine.2. Create a file named "token" in the <code>/var/lib/netapp/cloudinsights/acq/conf</code> folder on the AU.3. Click the <i>Copy Token</i> button, and paste this token into the file you created.4. Restart the AU service. Click the <i>Copy Restart Command</i> button, and paste the command into a command prompt on the AU.
Permission denied when starting the Acquisition Unit Server Service	When the AU is installed on SELINUX, SE should be set to <i>permissive</i> mode. <i>Enforcing</i> mode is not supported. After setting SELINUX to permissive mode, restart the AU service. Learn more .
Server Requirements not met	Ensure that your Acquisition Unit server or VM meets requirements
Network Requirements not met	<p>Ensure that your Acquisition Unit server/VM can access your Cloud Insights environment (<code><environment-name>.c01.cloudinsights.netapp.com</code>) through SSL connection over port 443. Try the following commands:</p> <pre>ping <environment-name>.c01.cloudinsights.netapp.com traceroute <environment-name>.c01.cloudinsights.netapp.com curl https://<environment-name>.c01.cloudinsights.netapp.com wget https://<environment-name>.c01.cloudinsights.netapp.com</pre>

Proxy Server not configured properly	<p>Verify your proxy settings, and uninstall/re-install the Acquisition Unit software if necessary to enter the correct proxy settings.</p> <ol style="list-style-type: none"> 1. Try "curl". Refer to "man curl" information/documentation regarding proxies: --proxy, --proxy-* (that's a wildcard "*" because curl supports many proxy settings). 2. Try "wget". Check documentation for proxy options.
Acquisition unit installation failed in Cloud insights with credential errors while starting acquisition service (and visible in the acq.log).	This can be caused by the inclusion of special characters in the proxy credentials. Uninstall the AU (<i>sudo cloudinsights-uninstall.sh</i>) and reinstall without using special characters.
Linux: missing library / file not found	Ensure that your Linux Acquisition Unit server/VM has all necessary libraries. For example, you must have the <i>unzip</i> library installed on the server. To install the <i>unzip</i> library, run the command <i>*sudo yum install unzip*</i> before running the Acquisition Unit install script
Permission issues	Be sure you are logged in as a user with <i>sudo</i> permissions
Acquisition Not Running:	Gather the acq.log from <i>/opt/netapp/cloudinsights/acq/logs</i> (Linux) Restart the Acquisition Service: <i>sudo cloudinsights-service.sh restart acquisition</i>
Data Collection Issues:	Send an Error Report from the Data Collector landing page by clicking the "Send Error Report" button
Status: Heartbeat Failed	<p>The Acquisition Unit (AU) sends a heartbeat to Cloud Insights every 60 seconds to renew its lease. If the heartbeat call fails due to network issue or unresponsive Cloud Insights, the AU's lease time isn't updated. When the AU's lease time expires, Cloud Insights shows a status of "Heartbeat Failed".</p> <p>Troubleshoot steps:</p> <p>Check the network connection between the Acquisition Unit sever and CloudInsights. Check whether the Acquisition Unit service is running. If the service is not running, start the service. Check the Acquisition Unit log (<i>/var/log/netapp/cloudinsights/acq/acq.log</i>) to see whether there are any errors.</p>
I'm seeing a "Heartbeat Error: message	This error can occur if there is a network interruption that causes communication between the Acquisition Unit and the Cloud Insights environment to be interrupted for more than one minute. Verify the connection between the AU and Cloud Insights is stable and active.

Considerations about Proxies and Firewalls

If your organization requires proxy usage for internet access, you may need to understand your organization's proxy behavior and seek certain exceptions for Cloud Insights to work. Keep the following in mind:

- First, does your organization block access by default, and only allow access to specific web sites/domains by exception? If so, you will need to get the following domain added to the exception list:

```
*.cloudinsights.netapp.com
```

Your Cloud Insights Acquisition Unit, as well as your interactions in a web browser with Cloud Insights, will all go to hosts with that domain name.

- Second, some proxies attempt to perform TLS/SSL inspection by impersonating Cloud Insights web sites with digital certificates not generated from NetApp. The Cloud Insights Acquisition Unit's security model is fundamentally incompatible with these technologies. You would also need the above domain name excepted from this functionality in order for the Cloud Insights Acquisition Unit to successfully login to Cloud Insights and facilitate data discovery.

In case where the proxy is set up for traffic inspection, the Cloud Insights environment must be added to an exception list in the proxy configuration. The format and setup of this exception list varies according to your proxy environment and tools, but in general you must add the URLs of the Cloud Insights servers to this exception list in order to allow the AU to properly communicate with those servers.

The simplest way to do this is to add the Cloud Insights domain itself to the exception list:

```
*.cloudinsights.netapp.com
```

In the case where the proxy is not set up for traffic inspection, an exception list may or may not be required. If you are unsure whether you need to add Cloud Insights to an exception list, or if you experience difficulties installing or running Cloud Insights due to proxy and/or firewall configuration, talk to your proxy administration team to set up the proxy's handling of SSL interception.

Viewing Proxy endpoints

You can view your proxy endpoints by clicking the **Proxy Settings** link when choosing a data collector during onboarding, or the link under *Proxy Settings* on the **Help > Support** page. A table like the following is displayed. If you have Workload Security in your environment, the configured endpoint URLs will also be displayed in this list.

If your organization requires proxy usage for internet access, you need to understand your organization's proxy behavior and seek certain exceptions for Cloud Insights to work. The simplest way is to add the following domains to the exception list:

Hostname	Port	Protocol	Methods	Endpoint URL Purpose
qtrjks0.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Tenant
00b1100.1234.abcd.a1b2c3ef56a7.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Ingestion
aulogin.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Authentication
portal.proxy.cloud.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Gateway

Close

Resources

Additional troubleshooting tips may be found in the [NetApp Knowledgebase](#) (support sign-in required).

Additional support information may be found from the Cloud Insights [Support](#) page.

Troubleshooting Acquisition Unit Problems on Windows

Here you will find suggestions for troubleshooting problems with Acquisition Units on a Windows server.

Problem:	Try this:
AU status on the Admin > Data Collectors page in the Acquisition Units tab displays "Certificate Expired" or "Certificate Revoked".	<p>Click on the menu to the right of the AU and select Restore Connection. Follow the instructions to restore your Acquisition Unit:</p> <ol style="list-style-type: none">1. Stop the Acquisition Unit (AU) service. You can click the <i>Copy Stop Command</i> button to quickly copy the command to the clipboard, then paste this command into a command prompt on the acquisition unit machine.2. Create a file named "token" in the <i>c:\Program Files\Cloud Insights\Acquisition Unit\conf</i> folder on the AU.3. Click the <i>Copy Token</i> button, and paste this token into the file you created.4. Restart the AU service. Click the <i>Copy Restart Command</i> button, and paste the command into a command prompt on the AU.
Server Requirements not met	Ensure that your Acquisition Unit server or VM meets requirements
Network Requirements not met	Ensure that your Acquisition Unit server/VM can access your Cloud Insights environment (<environment-name>.c01.cloudinsights.netapp.com) through SSL connection over port 443. Try the following commands: <i>ping <environment-name>.c01.cloudinsights.netapp.com traceroute <environment-name>.c01.cloudinsights.netapp.com curl https://<environment-name>.c01.cloudinsights.netapp.com wget https://<environment-name>.c01.cloudinsights.netapp.com</i>

Proxy Server not configured properly	<p>Verify your proxy settings, and uninstall/re-install the Acquisition Unit software if necessary to enter the correct proxy settings.</p> <ol style="list-style-type: none"> 1. Try "curl". Refer to "man curl" information/documentation regarding proxies: --proxy, --proxy-* (that's a wildcard "*" because curl supports many proxy settings). 2. Try "wget". Check documentation for proxy options.
Acquisition unit installation failed in Cloud insights with credential errors while starting acquisition service (and visible in the acq.log).	This can be caused by the inclusion of special characters in the proxy credentials. Uninstall the AU (<i>sudo cloudinsights-uninstall.sh</i>) and reinstall without using special characters.
Permission issues	Be sure you are logged in as a user with administrator permissions
Acquisition Not Running	You can find information in the acq.log in the <install directory>\Cloud Insights\Acquisition Unit\log folder. Restart the Acquisition via Windows Services
Data Collection Issues	Send an Error Report from the Data Collector landing page by clicking the "Send Error Report" button
Status: Heartbeat Failed	<p>The Acquisition Unit (AU) sends a heartbeat to Cloud Insights every 60 seconds to renew its lease. If the heartbeat call fails due to network issue or unresponsive Cloud Insights, the AU's lease time isn't updated. When the AU's lease time expires, Cloud Insights shows a status of "Heartbeat Failed".</p> <p>Troubleshoot steps:</p> <ul style="list-style-type: none"> * Check the network connection between the Acquisition Unit sever and CloudInsights. * Check whether the Acquisition Unit service is running. If the service is not running, start the service. * Check the Acquisition Unit log (<Install dir>:\Program Files\Cloud Insights\Acquisition Unit\log\acq.log) to see whether there are any errors.
I'm seeing a "Heartbeat Error: message	This error can occur if there is a network interruption that causes communication between the Acquisition Unit and the Cloud Insights environment to be interrupted for more than one minute. Verify the connection between the AU and Cloud Insights is stable and active.

Considerations about Proxies and Firewalls

If your organization requires proxy usage for internet access, you may need to understand your organization's proxy behavior and seek certain exceptions for Cloud Insights to work. Keep the following in mind:

- First, does your organization block access by default, and only allow access to specific web sites/domains by exception? If so, you will need to add the following domain to your exception list:

*.cloudinsights.netapp.com

Your Cloud Insights Acquisition Unit, as well as your interactions in a web browser with Cloud Insights, will all go to hosts with that domain name.

- Second, some proxies attempt to perform TLS/SSL inspection by impersonating Cloud Insights web sites with digital certificates not generated from NetApp. The Cloud Insights Acquisition Unit's security model is fundamentally incompatible with these technologies. You would also need the above domain name excepted from this functionality in order for the Cloud Insights Acquisition Unit to successfully login to Cloud Insights and facilitate data discovery.

Viewing Proxy endpoints

You can view your proxy endpoints by clicking the **Proxy Settings** link when choosing a data collector during onboarding, or the link under *Proxy Settings* on the **Help > Support** page. A table like the following is displayed. If you have Workload Security in your environment, the configured endpoint URLs will also be displayed in this list.

Proxy Settings					X
If your organization requires proxy usage for internet access, you need to understand your organization's proxy behavior and seek certain exceptions for Cloud Insights to work. The simplest way is to add the following domains to the exception list:					
Hostname	Port	Protocol	Methods	Endpoint URL Purpose	
qtrjks0.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Tenant	
00b1100.1234.abcd.12bc.a1b2c3ef56a7.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Ingestion	
aulogin.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Authentication	
portal.proxy.cloud.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Gateway	

Close

Resources

Additional troubleshooting tips may be found in the [NetApp Knowledgebase](#) (support sign-in required).

Additional support information may be found from the Cloud Insights [Support](#) page.

Researching a failed data collector

If a data collector has failure message and a High or Medium Impact, you need to research this problem using the data collector summary page with its linked information.

Use the following steps to determine the cause of failed data collectors. Data collector failure messages are displayed on the **Admin** menu and on the **Installed Data Collectors** page.

Steps

1. Click **Admin > Data Collectors > Installed Data Collectors**.
2. Click the linked Name of the failing data collector to open the Summary page.
3. On the Summary page, check the Comments area to read any notes that might have been left by another engineer who might also be investigating this failure.
4. Note any performance messages.
5. Move your mouse pointer over the segments of the Event Timeline graph to display additional information.
6. Select an error message for a Device and displayed below the Event Timeline and click the Error details icon that displays to the right of the message.

The Error details include the text of the error message, most likely causes, information in use, and suggestions of what can be tried to correct the problem.

7. In the Devices Reported By This Data Collector area, you might filter the list to display only devices of interest, and you can click the linked **Name** of a device to display the asset page for that device.
8. When you return to the data collector summary page, check the **Show Recent Changes** area at the bottom of the page to see if recent changes could have caused the problem.

Reference & Support

Requesting Support

You can access support options in Cloud Insights by clicking on **Help > Support**. The support options available to you depend on whether you are in Trial mode or Subscription mode.

<p>Cloud Insights Support</p> <p>NetApp Serial Number: 123456789011234567890 AWS Customer ID: AbCdEfGhI12345678990zyxWVU</p> <p>Support activation is required to enable support with NetApp through web ticket or phone. Activate Support at register.netapp.com.</p> <p><input checked="" type="checkbox"/> Check this box to allow NetApp access to your instance of Cloud Insights.</p>	<p>Contact Us</p> <p>Need help with Cloud Insights?</p> <p>Technical Support: Open a Support Ticket Phone (P1) Chat</p> <p>Sales: Have questions regarding your subscription? Contact Sales.</p>		
<p>Knowledge Base</p> <p>Search through the Cloud Insights Knowledge Base to find helpful articles.</p>	<p>Documentation Center</p> <p>Visit the Cloud Insights Documentation Center to find step by step instructions to help you get the most out of Cloud Insights.</p>	<p>Communities</p> <p>Join the Cloud Insights Community to follow ongoing discussions or create a new one.</p>	<p>Feedback</p> <p>We value your input. Your feedback helps us improve Cloud Insights.</p>
<p>Learning Center</p> <p>Cloud Insights Course List:</p> <ul style="list-style-type: none">• Hybrid Cloud Resource Management• Cloud Insights Fundamentals• Cloud Resource Management• Cloud Secure <p>Cloud Education All-Access Pass:</p> <p>Visit and subscribe the Cloud Education All-Access Pass to get unlimited access to our best cloud learning resources.</p> <p>Course Catalog:</p> <p>Browse the Learning Services Product Catalog to find all the courses that are relevant to you.</p>			
<p>Proxy Settings</p> <p>Need to setup proxy exceptions? Click here to learn more.</p>			



Activating support entitlement

Cloud Insights offers self-service and email support when running in trial mode. Once you have subscribed to the service, it is strongly recommended that you activate support entitlement. Activating support entitlement enables you to access technical support over the online chat, the web ticketing system, and the phone. The default support mode is self-service until registration is completed. See [details](#) below.

During the initial subscription process, your Cloud Insights instance will generate a 20-digit NetApp serial number starting with "950". This NetApp serial number represents the Cloud Insights subscription associated with your account. You must register the NetApp serial number to activate support entitlement. We offer two options for support registration:

1. User with pre-existing NetApp Support Site (NSS) SSO account (e.g. current NetApp customer)
2. New NetApp customer with no pre-existing NetApp Support Site (NSS) SSO account

Option 1: Steps for a user with a pre-existing NetApp Support Site (NSS) SSO account

Steps

1. Navigate to the NetApp registration website <https://register.netapp.com>
2. Select “I am already registered as NetApp Customer” and choose *Cloud Insights* as the Product Line. Select your Billing Provider (NetApp or AWS) and provide your Serial Number and your NetApp Subscription Name or AWS Customer ID by referring to the “Help > Support” menu within the Cloud Insights user interface:

Cloud Insights Support

NetApp Serial Number: 95011122233344455512 NetApp Subscription Name: A-000012345

Support activation is required to enable support with NetApp through chat, ticket or phone. Activate Support at register.netapp.com.

Check this box to allow NetApp access to your instance of Cloud Insights.

3. Complete the Existing Customer Registration form and click **Submit**.

Existing Customer Registration

The fields marked with * are mandatory

First Name*	Test
Last Name*	Cloud2
Company*	NetApp Inc. (VSA Only)
Email Address*	ng-cloudvol-csd1@netapp.com
Product Line*	Cloud Insights ▾
Billing Provider *	NetApp ▾
Cloud Insights Serial # *	e.g. 95012235021303893918
NetApp Subscription Name *	e.g. A-S0000100

Add another Serial #

4. If no errors occur, user will be directed to a “Registration Submitted Successfully” page. The email address associated with the NSS SSO username used for registration will receive an email within a couple minutes stating “your product is now eligible for support”.
5. This is a onetime registration for the Cloud Insights NetApp serial number.

Option 2: Steps for a new NetApp customer with no pre-existing NetApp Support Site (NSS) SSO account

Steps

1. Navigate to the NetApp registration website <https://register.netapp.com>
2. Select “I am not a registered NetApp Customer” and complete the required information in example form below:

New Customer Registration

IMPORTANT: After submitting, a confirmation email will be sent to the email address filled-in the form. Please click the validation link in that email to complete the registration.

The fields marked with * are mandatory

First Name*	<input type="text"/>
Last Name*	<input type="text"/>
Company*	<input type="text"/>
Email Address*	<input type="text"/>
Office Phone*	<input type="text"/>
Alternate Phone	<input type="text"/>
Address Line 1*	<input type="text"/>
Address Line 2	<input type="text"/>
Postal Code / City*	<input type="text"/> <input type="text"/>
State/Province / Country*	<input type="text"/> - Select - <input type="button" value="▼"/>
NetApp Reference SN	<input type="text"/>
If you currently own a NetApp product, please provide the Serial Number for that product here in order to speed-up the validation process	
Product Line*	<input type="text"/> Cloud Insights <input type="button" value="▼"/>
Billing Provider *	<input type="text"/> NetApp <input type="button" value="▼"/>
Cloud Insights Serial # * 	<input type="text"/> e.g. 95012235021303893918
NetApp Subscription Name * 	<input type="text"/> e.g. A-S0000100
Add another Serial #	

Security check:

Enter the characters shown in the image to verify your



1. Select *Cloud Insights* as the Product Line. Select your Billing Provider (NetApp or AWS) and provide your Serial Number and your NetApp Subscription Name or AWS Customer ID by referring to the “Help > Support” menu within the Cloud Insights user interface:

Cloud Insights Support

NetApp Serial Number:
9501112223344455512

NetApp Subscription Name:
A-000012345

Support activation is required to enable support with NetApp through chat, ticket or phone.
Activate Support at register.netapp.com.

Check this box to allow NetApp access to your instance of Cloud Insights.

2. If no errors occur, user will be directed to a “Registration Submitted Successfully” page. The email address associated with the NSS SSO username used for registration will receive an email within a few hours stating “your product is now eligible for support”.
3. As a new NetApp customer, you will also need to create a NetApp Support Site (NSS) user account for future registrations and access to support portal for technical support chat and web ticketing. This link is located at <https://mysupport.netapp.com/eservice/public/now.do>. You can provide your newly registered Cloud Insights serial number to expedite the process.
4. This is a one-time registration for the Cloud Insights NetApp serial number.

Obtaining Support Information

NetApp provides support for Cloud Insights in a variety of ways. Extensive free self-support options are available 24x7, such as knowledgebase (KB) articles or the NetApp community. For users who are subscribed to any of the Cloud Insights Editions (Basic*, Standard, Premium), technical support is available via phone or web ticketing. A NetApp Support Site (NSS) SSO account is required for web ticket along with case management.

*Support is available with Basic Edition as long as all your NetApp storage systems are covered at least at the Premium Support level.

Self-Service Support:

These support options are available in Trial mode and are available for free 24x7:

- **[Knowledgebase](#)**

Clicking the links in this section takes you to the NetApp Knowledgebase, where you can search through relevant articles, how-to's, and more.

- **[Documentation](#)**

Clicking on the Documentation link takes you to this documentation center.

- **[Community](#)**

Clicking on the community link takes you to the NetApp Cloud Insights community, where you can connect with peers and experts.

There is also a link to provide xref:/Feedback to help us improve Cloud Insights.

Subscription Support

In addition to the self-support options above, if you have a Cloud Insights subscription or paid support for monitored NetApp products or services, you can work with a NetApp Support Engineer to resolve your problem.



You must register in order to [activate support](#) for NetApp Cloud products. To register, go to NetApp's [Cloud Data Services Support Registration](#).

It is highly recommended that you check the box to allow a NetApp Support Engineer access to your Cloud Insights environment during your support session. This will allow the engineer to troubleshoot the problem and help you resolve it quickly. When your issue is resolved or your support session has ended, you can un-check the box.

You can request support by any of the following methods. You must have an active Cloud Insights subscription to use these support options:

- [Phone](#)
- [Support Ticket](#)
- **Chat** - You will be connected with NetApp support personnel for assistance (weekdays only). Chat is available in the **Help > Live Chat** menu option in the upper right of any Cloud Insights screen.

You can also request sales support by clicking on the [Contact Sales](#) link.

Your Cloud Insights serial number is visible within the service from the **Help > Support** menu. If you are experiencing issues accessing the service and have registered a serial number with NetApp previously, you can also view your list of Cloud Insights serial numbers from the NetApp Support Site as follows:

- Login to mysupport.netapp.com
- From the Products > My Products menu tab, use Product Family "SaaS Cloud Insights" to locate all your registered serial numbers:

View Installed Systems

Selection Criteria

► Select: Serial Number (located on back of unit) Then, enter Value: Go!
Enter the entire value, or use asterisk (*) for wildcard searches. (Wildcard search does not apply to Serial Numbers)
Wildcard searches may take some time.
Enter the Cluster Serial Number value without dashes.

- OR -

► Search Type*: Product Family (optional):
 Serial Numbers for My Location SAAS CLOUD INSIGHTS
City (optional): State/Province (optional): US and Canada Only
Postal Code (optional): Country (optional): - Select One - Go!

Details

If you see any discrepancies or errors in the information shown below, please submit [Feedback](#) and be sure to include the serial nu

Cloud Insights Data Collector Support Matrix

You can view or download information and details about supported Data Collectors in the [Cloud Insights Data Collector Support Matrix](#).

Learning Center

Regardless of your subscription, **Help > Support** links to several NetApp University course offerings to help you get the most out of Cloud Insights. Check them out!

Cloud Insights Data Collector Support Matrix

The Data Collector Support Matrix provides reference for Data Collectors supported by cloud Insights, including vendor and model information.

The matrix is provided in .PDF format.

Click the link to open.

Right-click and choose Save as... to download a copy.

[Data Collector Support Matrix](#)

Data Collector Reference - Infrastructure

Vendor-Specific Reference

The topics in this section provide vendor-specific reference information. In most cases, configuring a data collector is straightforward. In some cases, you may need additional information or commands to properly configure the data collector.

Click on a **vendor** in the menu to the left to see information for their data collectors.

Configuring the Amazon EC2 data collector

Cloud Insights uses the Amazon EC2 data collector to acquire inventory and performance data from EC2 instances.

Requirements

In order to collect data from Amazon EC2 devices, you must have the following information:

- You must have one of the following:
 - The **IAM Role** for your Amazon EC2 cloud account, if using IAM Role Authentication. IAM Role only applies if your acquisition unit is installed on an AWS instance.
 - The **IAM Access Key ID** and Secret Access Key for your Amazon EC2 cloud account, if using IAM Access Key authentication.
- You must have the "list organization" privilege
- Port 443 HTTPS
- EC2 Instances can be reported as a Virtual Machine, or (less naturally) a Host. EBS Volumes can be reported as both a VirtualDisk used by the VM, as well as a DataStore providing the Capacity for the VirtualDisk.

Access keys consist of an access key ID (for example, AKIAIOSFODNN7EXAMPLE) and a secret access key (for example, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY). You use access keys to sign programmatic requests that you make to EC2 if you use the Amazon EC2 SDKs, REST, or Query API operations. These keys are provided with your contract from Amazon.

Configuration

Enter data into the data collector fields according to the table below:

Field	Description
AWS Region	Choose AWS region
IAM Role	For use only when acquired on an AU in AWS. See below for more information on IAM Roles .
AWS IAM Access Key ID	Enter AWS IAM Access Key ID. Required if you do not use IAM Role.

Field	Description
AWS IAM Secret Access Key	Enter AWS IAM Secret Access Key. Required if you do not use IAM Role.
I understand AWS bills me for API requests	Check this to verify your understanding that AWS bills you for API requests made by Cloud Insights polling.

Advanced Configuration

Field	Description
Include Extra Regions	Specify additional regions to include in polling.
Cross Account Role	Role for accessing resources in different AWS accounts.
Inventory Poll Interval (min)	The default is 60
Choose 'Exclude' or 'Include' to Apply to Filter VMs by Tags	Specify whether to include or exclude VM's by Tags when collecting data. If 'Include' is selected, the Tag Key field can not be empty.
Tag Keys and Values on which to Filter VMs	Click + Filter Tag to choose which VMs (and associated disks) to include/exclude by filtering for keys and values that match keys and values of tags on the VM. Tag Key is required, Tag Value is optional. When Tag Value is empty, the VM is filtered as long as it matches the Tag Key.
Performance Poll Interval (sec)	The default is 1800
CloudWatch Agent Metrics Namespace	Namespace in EC2/EBS from which to collect data. Note that if the names of the default metrics in this namespace are changed, Cloud Insights may not be able to collect that renamed data. It is recommended to leave the default metric names.

IAM Access Key

Access keys are long-term credentials for an IAM user or the AWS account root user. Access keys are used to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK).

Access keys consist of two parts: an access key ID and a secret access key. When you use *IAM Access Key* authentication (as opposed to *IAM Role* authentication), you must use both the access key ID and secret access key together for authentication of requests. For more information, see the Amazon documentation on [Access Keys](#).

IAM Role

When using *IAM Role* authentication (as opposed to IAM Access Key authentication), you must ensure that the role you create or specify has the appropriate permissions needed to access your resources.

For example, if you create an IAM role named *InstanceEc2ReadOnly*, you must set up the policy to grant EC2 read-only list access permission to all EC2 resources for this IAM role. Additionally, you must grant STS (Security Token Service) access so that this role is allowed to assume roles cross accounts.

After you create an IAM role, you can attach it when you create a new EC2 instance or any existing EC2 instance.

After you attach the IAM role *InstanceEc2ReadOnly* to an EC2 instance, you will be able to retrieve the temporary credential through instance metadata by IAM role name and use it to access AWS resources by any application running on this EC2 instance.

For more information see the Amazon documentaiton on [IAM Roles](#).

Note: IAM role can be used only when the Acquisition Unit is running in an AWS instance.

Mapping Amazon tags to Cloud Insights annotations

The Amazon EC2 data collector includes an option that allows you to populate Cloud Insights annotations with tags configured on EC2. The annotations must be named exactly as the EC2 tags. Cloud Insights will always populate same-named text-type annotations, and will make a "best attempt" to populate annotations of other types (number, boolean, etc). If your annotation is of a different type and the data collector fails to populate it, it may be necessary to remove the annotation and re-create it as a text type.

Note that AWS is case-sensitive, while Cloud Insights is case-insensitive. So if you create an annotation named "OWNER" in Cloud Insights, and tags named "OWNER", "Owner", and "owner" in EC2, all of the EC2 variations of "owner" will map to Cloud Insight's "OWNER" annotation.

Include Extra Regions

In the AWS Data Collector **Advanced Configuration** section, you can set the **Include extra regions** field to include additional regions, separated by comma or semi-colon. By default, this field is set to **us-***, which collects on all US AWS regions. To collect on *all* regions, set this field to ***.***.

If the **Include extra regions** field is empty, the data collector will collect on assets specified in the **AWS Region** field as specified in the **Configuration** section.

Collecting from AWS Child Accounts

Cloud Insights supports collection of child accounts for AWS within a single AWS data collector. Configuration for this collection is performed in the AWS environment:

- You must configure each child account to have an AWS Role that allows the main account ID to access EC2 details from the children account.
- Each child account must have the role name configured as the same string.
- Enter this role name string into the Cloud Insights AWS Data Collector **Advanced Configuration** section, in the **Cross account role** field.

Best Practice: It is highly recommended to assign the AWS predefined *AmazonEC2ReadOnlyAccess* policy to the EC2 main account. Also, the user configured in the data source should have at least the predefined *AWSOrganizationsReadOnlyAccess* policy assigned, in order to query AWS.

Please see the following for information on configuring your environment to allow Cloud Insights to collect from AWS child accounts:

[Tutorial: Delegate Access Across AWS Accounts Using IAM Roles](#)

[AWS Setup: Providing Access to an IAM User in Another AWS Account That You Own](#)

Troubleshooting

Additional information on this Data Collector may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Amazon FSx for NetApp ONTAP data collector

This data collector acquires inventory and performance data from Amazon FSx for NetApp ONTAP. This data collector will be made available incrementally throughout the Cloud Insights service regions. Contact your sales person if you do not see the icon for this collector in your Cloud Insights Environment.

Terminology

Cloud Insights acquires inventory and performance data from the FSx-NetApp data collector. For each asset type acquired, the most common terminology used for the asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Cluster	Storage
LUN	Volume
Volume	Internal Volume

FSx-NetApp Terminology

The following terms apply to objects or references that you might find on FSx-NetApp storage asset landing pages. Many of these terms apply to other data collectors as well.

Storage

- Model – A comma-delimited list of the unique, discrete model names within this cluster.
- Vendor – AWS
- Serial number – The array serial number.
- IP – generally will be the IP(s) or hostname(s) as configured in the data source.
- Raw Capacity – base 2 summation of all the SSD storage assigned to the FSx filesystem.
- Latency – a representation of what the host facing workloads are experiencing, across both reads and writes. Ideally, Cloud Insights is sourcing this value directly, but this is often not the case. In lieu of the array offering this up, Cloud Insights is generally performing an IOPs-weighted calculation derived from the individual internal volumes' statistics.
- Throughput – aggregated from internal volumes.
Management – this may contain a hyperlink for the management interface of the device. Created programmatically by the Cloud Insights data source as part of inventory reporting.

Storage Pool

- Storage – what storage array this pool lives on. Mandatory.
- Type – a descriptive value from a list of an enumerated list of possibilities. Most commonly will be “Aggregate” or “RAID Group”.
- Capacity – the values here are the logical used, usable capacity and the logical total capacity, and the percentage used across these.
- IOPS – the sum IOPs of all the volumes allocated on this storage pool.
- Throughput – the sum throughput of all the volumes allocated on this storage pool.

Requirements

The following are requirements to configure and use this data collector:

- You must have access to an Administrator account configured for read-only API calls.
- Account details include username and password.
- Port requirements: 80 or 443

Configuration

Field	Description
NetApp Management IP	IP address or fully-qualified domain name of the NetApp cluster
User Name	User name for NetApp cluster
Password	Password for NetApp cluster

Advanced Metrics

This data collector collects the following advanced metrics from the FSx for NetApp ONTAP storage:

- fpolicy
- nfsv3
- nfsv3:node
- nfsv4
- nfsv4_1
- nfsv4_1:node
- nfsv4:node
- policy_group
- qtree
- volume
- workload_volume

Troubleshooting

Some things to try if you encounter problems with this data collector:

Inventory

Problem:	Try this:
Receive 401 HTTP response or 13003 ZAPI error code and ZAPI returns “Insufficient privileges” or “not authorized for this command”	Check username and password, and user privileges/permissions.
ZAPI returns "cluster role is not cluster_mgmt LIF"	AU needs to talk to cluster management IP. Check the IP and change to a different IP if necessary
ZAPI command fails after retry	AU has communication problem with the cluster. Check network, port number, and IP address. User should also try to run a command from command line from the AU machine.
AU failed to connect to ZAPI via HTTP	Check whether ZAPI port accepts plaintext. If AU tries to send plaintext to an SSL socket, the communication fails.
Communication fails with SSLEException	AU is attempting to send SSL to a plaintext port on a filer. Check whether the ZAPI port accepts SSL, or use a different port.
Additional Connection errors: ZAPI response has error code 13001, “database is not open” ZAPI error code is 60 and response contains “API did not finish on time” ZAPI response contains “initialize_session() returned NULL environment” ZAPI error code is 14007 and response contains “Node is not healthy”	Check network, port number, and IP address. User should also try to run a command from command line from the AU machine.

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Configuring the Azure compute data collector

Cloud Insights uses the Azure compute data collector to acquire inventory and performance data from Azure compute instances.

Requirements

You need the following information to configure this data collector.

- Port requirement: 443 HTTPS

- Azure OAuth 2.0 Redirect URI (login.microsoftonline.com)
- Azure Management Rest IP (management.azure.com)
- Azure Resource Manager IP (management.core.windows.net)
- Azure Service Principal Application (Client) ID (Reader role required)
- Azure service principal authentication key (user password)
- You need to set up an Azure account for Cloud Insights discovery.

Once the account is properly configured and you register the application in Azure, you will have the credentials required to discover the Azure instance with Cloud Insights. The following link describes how to set up the account for discovery.

<https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal>

Configuration

Enter data into the data collector fields according to the table below:

Field	Description
Azure Service Principal Application (Client) ID (Reader role required)	Sign-in ID to Azure. Requires Reader Role access.
Azure tenant ID	Microsoft tenant ID
Azure Service Principal Authentication Key	Login authentication key
I understand Microsoft bills me for API requests	Check this to verify your understanding that Microsoft bills you for API requests made by Insight polling.

Advanced Configuration

Field	Description
Inventory Poll Interval (min)	The default is 60
Choose 'Exclude' or 'Include' to Apply to Filter VMs by Tags	Specify whether to include or exclude VM's by Tags when collecting data. If 'Include' is selected, the Tag Key field can not be empty.
Tag Keys and Values on which to Filter VMs	Click + Filter Tag to choose which VMs (and associated disks) to include/exclude by filtering for keys and values that match keys and values of tags on the VM. Tag Key is required, Tag Value is optional. When Tag Value is empty, the VM is filtered as long as it matches the Tag Key.
Performance Poll Interval (sec)	The default is 300

Troubleshooting

Additional information on this Data Collector may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Broadcom

Brocade Network Advisor data collector

Cloud Insights uses the Brocade Network Advisor data collector to acquire inventory and performance data from Brocade switches.

Terminology

Cloud Insights acquires the following inventory information from the Brocade Network Advisor data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Switch	Switch
Port	Port
Virtual Fabric, Physical Fabric	Fabric
Logical Switch	Logical Switch

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

The following are required to configure this data collector:

- The Cloud Insights Acquisition Unit will initiate connections to TCP port 443 on the BNA server. BNA server must be running version 14.2.1 or higher.
- Brocade Network Advisor Server IP address
- User name and password to an administrator account
- Port requirement: HTTP/HTTPS 443

Configuration

Field	Description
Brocade Network Advisor Server IP	IP address of the Network Advisor Server
User Name	User name for the switch
User Name	Administrator user name
Password	Administrator password

Advanced configuration

Field	Description
Connection Type	HTTPS (default port 443) or HTTP (default port 80)

Field	Description
Override Connection Port	If blank, use the default port in the Connection Type field, otherwise enter the connection port to use
Password	Password for the switch
Inventory poll interval (min)	The default is 40
Report Access Gateway	Check to include devices in Access Gateway mode
Performance Poll Interval (sec)	The default is 1800

Troubleshooting

Some things to try if you encounter problems with this data collector:

Inventory

Problem:	Try this:
Receive a message that more than 1 node is logged into the Access Gateway port, or data collector fails to discover Access Gateway device.	Check that the NPV device is operating correctly and that all connected WWNs are expected. Do not directly acquire the NPV device. Instead, acquisition of the core fabric switch will collect the NPV device data.

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Brocade FC Switch data collector

Cloud Insights uses the Brocade FC Switch (SSH) data source to discover inventory for Brocade or rebranded switch devices running Factored Operating System (FOS) firmware 4.2 and later. Devices in both FC switch and Access Gateway modes are supported.

Terminology

Cloud Insights acquires the following inventory information from the Brocade FC Switch data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Switch	Switch
Port	Port
Virtual Fabric, Physical Fabric	Fabric
Zone	Zone
Logical Switch	Logical Switch
Virtual Volume	Volume
LSAN Zone	IVR Zone

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

- The Cloud Insights Acquisition Unit (AU) will initiate connections to TCP Port 22 on Brocade switches to collect inventory data. The AU will also initiate connections to UDP port 161 for collection of performance data.
- There must be IP connectivity to all switches in the fabric. If you select the Discover all switches in the fabric check box, Cloud Insights identifies all the switches in the fabric; however, it needs IP connectivity to these additional switches to discover them.
- The same account is needed globally across all switches in the fabric. You can use PuTTY (open source terminal emulator) to confirm access.
- Ports 161 and 162 must be open to all switches in the fabric for SNMP performance polling.
- SNMP read-only Community String

Configuration

Field	Description
Switch IP	IP address or fully-qualified domain name of the EFC Server
User Name	User name for the switch
Password	Password for the switch
SNMP	SNMP version
SNMP Community String	SNMP read-only community string used to access the switch
SNMP User Name	SNMP user name
SNMP Password	SNMP password

Advanced configuration

Field	Description
Fabric name	Fabric name to be reported by the data collector. Leave blank to report the fabric name as WWN.
Inventory Poll Interval (min)	Interval between inventory polls. The default is 15.
Excluded Devices	Comma-separated list of device IDs to exclude from polling
Admin Domains Active	Select if using Admin Domains
Retrieve MPR Data	Select to acquire routing data from your multiprotocol router.
Enable Trapping	Select to enable acquisition upon receiving an SNMP trap from the device. If you select enable trapping, you must also activate SNMP.

Field	Description
Minimum Time Between Traps (sec)	Minimum time between acquisition attempts triggered by traps. The default is 10.
Discover all switches in the fabric	Select to discover all switches in the fabric
Choose Favoring HBA vs. Zone Aliases	Choose whether to favor HBA or zone aliases
Performance Poll Interval (sec)	Interval between performance polls. The default is 300.
SNMP Auth Protocol	SNMP authentication protocol (SNMP v3 only)
SNMP Privacy Password	SNMP privacy password (SNMP v3 only)
SNMP Retries	Number of SNMP retry attempts

Troubleshooting

Some things to try if you encounter problems with this data collector:

Inventory

Problem:	Try this:
The inventory acquisition of the Brocade datasource fails with the error: <pre><date> <time> ERROR [com.onaro.sanscreen.acquisition.framework.datasouce.BaseDataSource] Error 2 out of 2: <datasource name> [Internal error] - Unable to generate the model for device <IP>. Error detecting prompt ([Device name <name>]: Unable to generate the model for device <IP>. Error detecting prompt)</pre>	The issue may be caused when the Brocade switch takes too long to return with a prompt, exceeding the default timeout of 5 seconds. In the data collector's Advanced Configuration settings in Cloud Insights, try increasing the <i>SSH Banner Wait Timeout (sec)</i> to a higher value.
Error: "Cloud Insights received Invalid Chassis Role"	Check that the user configured in this data source has been granted the chassis role permission.
Error: "Mismatched Chassis IP Address"	Change the data source configuration to use chassis IP address.
Receive a message that more than 1 node is logged into the Access Gateway port	Check that the NPV device is operating correctly and that all connected WWNs are expected. Do not directly acquire the NPV device. Instead, acquisition of the core fabric switch will collect the NPV device data.

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Cisco MDS Fabric Switches data collector

Cloud Insights uses the Cisco MDS Fabric Switches data collector to discover inventory for Cisco MDS Fabric Switches as well as a variety of Cisco Nexus FCoE switches on which the FC service is enabled.

Additionally, you can discover many models of Cisco devices running in NPV mode with this data collector.

Terminology

Cloud Insights acquires the following inventory information from the Cisco FC Switch data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Switch	Switch
Port	Port
VSAN	Fabric
Zone	Zone
Logical Switch	Logical Switch
Name Server Entry	Name Server Entry
Inter-VSAN Routing (IVR) Zone	IVR Zone

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

- An IP address of one switch in the fabric or individual switches
- Chassis discovery, to enable fabric discovery
- If using SNMP V2, read-only community string
- Port 161 is used to access the device

Configuration

Field	Description
Cisco Switch IP	IP address or fully-qualified domain name of the switch
SNMP Version	Select V1, V2, or V3. V2 or later is required for performance acquisition.
SNMP Community String	SNMP read-only community string used to access the switch (not applicable for SNMP v3)
User Name	User name for the switch (SNMP v3 only)
Password	Password used for the switch (SNMPv3 only)

Advanced configuration

Field	Description
Inventory Poll Interval (min)	Interval between inventory polls (default 40 minutes)

Field	Description
SNMP Auth Protocol	SNMP authentication protocol (SNMPv3 only)
SNMP Privacy Protocol	SNMP privacy protocol (SNMPv3 only)
SNMP Privacy Password	SNMP Privacy Password
SNMP Retries	Number of SNMP retry attempts
SNMP Timeout (ms)	SNMP timeout (default 5000 ms)
Enable Trapping	Select to enable trapping. If you enable trapping, you must also activate SNMP notifications.
Minimum Time Between Traps (sec)	Minimum time between acquisition attempts triggered by traps (default 10 seconds)
Discover All Fabric Switches	Select to discover all switches in the fabric
Excluded Devices	Comma-separated list of device IPs to exclude from polling
Included Devices	Comma-separated list of device IPs to include in polling
Check Device Type	Select to accept only those devices that explicitly advertise themselves as Cisco devices
First Alias Type	<p>Provide a first preference for resolution of the alias. Choose from the following:</p> <p>Device Alias This is a user-friendly name for a port WWN (pWWN) that can be used in all configuration commands, as required. All switches in the Cisco MDS 9000 Family support Distributed Device Alias Services (device aliases).</p> <p>None Do not report any alias.</p> <p>Port Description A description to help identify the port in a list of ports.</p> <p>Zone Alias (all) A user-friendly name for a port that can be used only for the active configuration. This is the default.</p>
Second Alias Type	Provide a second preference for resolution of the alias
Third Alias Type	Provide a third preference for resolution of the alias
Enable SANTap Proxy Mode Support	Select if your Cisco switch is using SANTap in proxy mode. If you are using EMC RecoverPoint, then you are probably using SANTap.
Performance Poll Interval (sec)	Interval between performance polls (default 300 seconds)

Troubleshooting

Some things to try if you encounter problems with this data collector:

Inventory

Problem:	Try this:
Error: Failed to discover chassis - no switches have been discovered	<ul style="list-style-type: none">• Ping the device with the IP configured• Login to the device using Cisco Device Manager GUI• Login to the device using CLI• Try to run SNMP walk
Error: Device is not a Cisco MDS switch	<ul style="list-style-type: none">• Make sure the data source IP configured for the device is correct• Login to the device using Cisco Device Manager GUI• Login to the device using CLI
Error: Cloud Insights is not able to obtain the switch's WWN.	This may not be a FC or FCoE switch, and as such may not be supported. Make sure the IP/FQDN configured in the datasource is truly a FC/FCoE switch.
Error: Found more than one nodes logged into NPV switch port	Disable direct acquisition of the NPV switch
Error: Could not connect to the switch	<ul style="list-style-type: none">• Make sure the device is UP• Check the IP address and listening port• Ping the device• Login to the device using Cisco Device Manager GUI• Login to the device using CLI• Run SNMP walk

Performance

Problem:	Try this:
Error: Performance acquisition not supported by SNMP v1	<ul style="list-style-type: none">• Edit Data Source and disable Switch Performance• Modify Data Source and switch configuration to use SNMP v2 or higher

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Cohesity SmartFiles data collector

This REST API-based collector will acquire a Cohesity cluster, discovering the “Views” (as Cloud Insights Internal Volumes), the various nodes, as well as collecting performance metrics.

Configuration

Field	Description
Cohesity Cluster IP	IP address of the Cohesity cluster

Field	Description
User Name	User name for the Cohesity cluster
Password	Password used for the Cohesity cluster

Advanced configuration

Field	Description
TCP Port	Port used for TCP communication with the Cohesity cluster
Inventory Poll Interval (min)	Interval between inventory polls. The default is 60 minutes.
Performance Poll Interval (min)	Interval between performance polls. The default is 900 seconds.

Troubleshooting

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Dell

Dell EMC XC Series data collector

Cloud Insights uses this data collector to discover inventory and performance information for the Dell EMC XC Series storage arrays.

Configuration

Field	Description
Prism External IP Address	IP address of the XC server
User Name	User name for the XC server
Password	Password used for the XC server

Advanced configuration

Field	Description
TCP Port	Port used for TCP communication with the XC server
Inventory Poll Interval (min)	Interval between inventory polls. The default is 60 minutes.
Performance Poll Interval (min)	Interval between performance polls. The default is 300 seconds.

Troubleshooting

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Dell EMC

DELL EMC Data Domain data collector

This data collector gathers inventory and performance information from DELL EMC Data Domain deduplication storage systems. To configure this data collector, there are specific configuration instructions and usage recommendations you must follow.

Terminology

Cloud Insights acquires the following inventory information from the Data Domain data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Disk	Disk
Array	Storage
FC Port	Port
File System	Internal Volume
Quota	Quota
NFS and CIFS share	FileShare

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

You need the following information to configure this data collector:

- IP address of the Data Domain device
- Read-only user name and password to the Data Domain storage
- SSH port 22

Configuration

Field	Description
IP address	The IP address or fully-qualified domain name of the Data Domain storage array
User name	The user name for the Data Domain storage array
Password	The password for the Data Domain storage array

Advanced configuration

Field	Description
Inventory Poll Interval (min)	Interval between inventory polls. The default is 20.
SSH Port	SSH service port

Troubleshooting

Additional information on this Data Collector may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Configuring the EMC ECS data collector

This data collector acquires inventory and performance data from EMC ECS storage systems. For configuration, the data collector requires an IP address of the ECS server and an administrative level domain account.



Dell EMC ECS is metered at a different Raw TB to Managed Unit rate. Every 40 TB of unformatted ECS capacity is charged as 1 [Managed Unit \(MU\)](#).

Terminology

Cloud Insights acquires the following inventory information from the ECS data collector. For each asset type acquired, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Cluster	Storage
Tenant	Storage Pool
Bucket	Internal Volume
Disk	Disk

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

- An IP address of the ECS Management Console
- Administrative level domain account for the ECS system
- Port 443 (HTTPS). Requires outbound connectivity to TCP port 443 on the ECS system.
- For performance, read-only username and password for ssh/scp access.
- For performance, port 22 is required.

Configuration

Field	Description
ECS Host	IP address or fully-qualified domain name of the ECS system
ECS Host Port	Port used for communication with ECS Host
ECS Vendor ID	Vendor ID for ECS
Password	Password used for ECS

Advanced configuration

Field	Description
Inventory Poll Interval (min)	The default is 360 minutes.

Troubleshooting

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Dell EMC PowerScale data collector

Cloud Insights uses the Dell EMC PowerScale (previously Isilon) SSH data collector to acquire inventory and performance data from PowerScale scale-out NAS storage.

Terminology

Cloud Insights acquires the following inventory information from this data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Drive	Disk
Cluster	Storage
Node	Storage Node
File System	Internal Volume

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

You need the following information to configure this data collector:

- Administrator permissions to the PowerScale storage
- IP address of the PowerScale cluster
- SSH access to port 22

Configuration

Field	Description
IP address	The IP address or fully-qualified domain name of the PowerScale cluster
User Name	User name for the PowerScale cluster
Password	Password used for the PowerScale cluster

Advanced configuration

Field	Description
Inventory Poll Interval (min)	Interval between inventory polls. The default is 20.
Performance Poll Interval (sec)	Interval between performance polls. The default is 300.
SSH Port	SSH service port. The default is 22.

Troubleshooting

Some things to try if you encounter problems with this data collector:

Inventory

Problem:	Try this:
"Invalid login credentials" with error messages "Commands not enabled for role-based administration require root user access"	* Verify that the user has permissions to run the following commands on the device: > isi version osrelease > isi status -q > isi status -n > isi devices -d %s > isi license * Verify credentials used in the wizard are matching device credentials
"Internal Error" with error messages "Command <Your command> run failed with permission: <Your current permission>. Sudo command run permission issue"	Verify that the user has sudo permissions to run the following command on the device

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Dell EMC Isilon / PowerScale REST data collector

Cloud Insights uses the Dell EMC Isilon / PowerScale REST data collector to acquire inventory and performance data from Dell EMC Isilon or PowerScale storage.

Terminology

Cloud Insights acquires the following inventory information from this data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Drive	Disk
Cluster	Storage
Node	Storage Node
OneFS File System	Internal Volume
OneFS File System	Storage Pool
Qtree	Qtree

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

You need the following information to configure this data collector:

- A user account and password. This account does NOT need to be admin/root, but you MUST grant a substantial number of read only privileges to your service account - see table below
- IP address / Fully Qualified Domain Name of the Dell EMC Isilon / PowerScale cluster
- HTTPS access to port 8080

Privilege Name	Description	r(read) or rw (read+write)
ISI_PRIV_LOGIN_PAPI	Platform API	r
ISI_PRIV_SYS_TIME	Time	r
ISI_PRIV_AUTH	Auth	r
ISI_PRIV_ROLE	Privilege	r
ISI_PRIV_DEVICES	Devices	r
ISI_PRIV_EVENT	Event	r
ISI_PRIV_HDFS	HDFS	r
ISI_PRIV_NDMP	NDMP	r
ISI_PRIV_NETWORK	Network	r
ISI_PRIV_NFS	NFS	r
ISI_PRIV_PAPI_CONFIG	Configure Platform API	r
ISI_PRIV_QUOTA	Quota	r
ISI_PRIV_SMARTPOOLS	SmartPools	r
ISI_PRIV_SMB	SMB	r
ISI_PRIV_STATISTICS	Statistics	r
ISI_PRIV_SWIFT	Swift	r
ISI_PRIV_JOB_ENGINE	Job Engine	r

Configuration

Field	Description
Isilon IP address	The IP address or fully-qualified domain name of the Isilon storage
User Name	User name for the Isilon
Password	Password used for the Isilon

Advanced configuration

Field	Description
HTTPS Port	The default is 8080.
Inventory Poll Interval (min)	Interval between inventory polls. The default is 20.
Performance Poll Interval (sec)	Interval between performance polls. The default is 300.

Troubleshooting

Some things to try if you encounter problems with this data collector:

Inventory

Problem:	Try this:
"Invalid login credentials" with error messages "Commands not enabled for role-based administration require root user access"	* Verify that the user has permissions to run the following commands on the device: > isi version osrelease > isi status -q > isi status -n > isi devices -d %s > isi license * Verify credentials used in the wizard are matching device credentials
"Internal Error" with error messages "Command <Your command> run failed with permission: <Your current permission>. Sudo command run permission issue"	Verify that the user has sudo permissions to run the following command on the device

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Dell EMC PowerStore data collector

The EMC PowerStore data collector gathers inventory information from EMC PowerStore storage. For configuration, the data collector requires the IP address of the storage processors and a read-only user name and password.

The EMC PowerStore data collector gathers the volume-to-volume replication relationships that PowerStore coordinates across other storage arrays. Cloud Insights shows a storage array for each PowerStore cluster, and collects inventory data for nodes and storage ports on that cluster. No storage pool or volume data is

collected.

Terminology

Cloud Insights acquires the following inventory information from this data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
host	host
host_volume_mapping	host_volume_mapping
hardware (it has Drives under "extra_details" object): Drives	Disk
Appliance	StoragePool
Cluster	Storage Array
Node	StorageNode
fc_port	Port
volume	Volume
InternalVolume	file_system

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

The following information is required to configure this data collector:

- IP address or fully-qualified domain name of storage processor
- Read-only user name and password

Configuration

Field	Description
PowerStore gateway(s)	IP addresses or fully-qualified domain names of PowerStore storage
User Name	User name for PowerStore
Password	Password used for PowerStore

Advanced configuration

Field	Description
HTTPS Port	Default is 443
Inventory Poll Interval (minutes)	Interval between inventory polls. The default is 60 minutes.

Cloud Insight's PowerStore performance collection makes use of PowerStore's 5-minute granularity source data. As such, Cloud Insights polls for that data every five minutes, and this is not configurable.

Troubleshooting

Additional information on this Data Collector may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Dell EMC RecoverPoint data collector

The EMC RecoverPoint data collector's primary use case is to discover volume-to-volume replication relationships that the RecoverPoint storage appliance facilitates. This collector will also discover the Recoverpoint appliance itself. Please note that Dell/EMC sells a VMware backup solution for VMs--"RecoverPoint for VMs"--which is not supported by this collector

For configuration, the data collector requires the IP address of the storage processors and a read-only user name and password.

The EMC RecoverPoint data collector gathers the volume-to-volume replication relationships that RecoverPoint coordinates across other storage arrays. Cloud Insights shows a storage array for each RecoverPoint cluster, and collects inventory data for nodes and storage ports on that cluster. No storage pool or volume data is collected.

Requirements

The following information is required to configure this data collector:

- IP address or fully-qualified domain name of storage processor
- Read-only user name and password
- REST API access via port 443

Configuration

Field	Description
Address of RecoverPoint	IP address or fully-qualified domain name of RecoverPoint cluster
User Name	User name for the RecoverPoint cluster
Password	Password used for the RecoverPoint cluster

Advanced configuration

Field	Description
TCP Port	TCP Port used to connect to Recoverpoint cluster
Inventory Poll Interval (minutes)	Interval between inventory polls. The default is 20 minutes.

Field	Description
Excluded Clusters	Comma-separated list of cluster IDs or names to exclude when polling.

Troubleshooting

Additional information on this Data Collector may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

DELL EMC ScaleIO data collector

The ScaleIO data collector collects inventory information from ScaleIO storage. For configuration, this data collector requires the ScaleIO gateway address and an admin user name and password.

Terminology

Cloud Insights acquires the following inventory information from the ScaleIO data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
MDM (Meta Data Manager) Cluster	Storage
SDS (ScaleIO Data Server)	Storage Node
Storage Pool	Storage Pool
Volume	Volume
Device	Disk

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

- Read-only access to the Admin user account
- Port requirement: HTTPS Port 443

Configuration

Field	Description
ScaleIO Gateway(s)	IP addresses or FQDNs of ScaleIO gateways, separated by comma (,) or semicolon (;)
User Name	Admin user name used to log in to the ScaleIO device
Password	Password used to log in to the ScaleIO device

Advanced configuration

Click the Inventory check box to enable inventory collection.

Field	Description
HTTPS port	443
Inventory poll interval (min)	The default is 60.
Connection Timeout (sec)	The default is 60.

Troubleshooting

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Configuring the EMC Unity data collector

The DELL EMC Unity (formerly VNXe) data collector provides inventory support for VNXe unified storage arrays. Cloud Insights currently supports iSCSI and NAS protocols.

Requirements

- The Unity data collector is CLI based; you must install the Unisphere for Unity CLI, (uemcli.exe) onto the acquisition unit where your VNXe data collector resides.
- uemcli.exe uses HTTPS as the transport protocol, so the acquisition unit will need to be able to initiate HTTPS connections to the Unity.
- IP address or fully-qualified domain name of the Unity device
- You must have at least a read-only user for use by the data collector.
- HTTPS on Port 443 is required
- The EMC Unity data collector provides NAS and iSCSI support for inventory; fibre channel volumes will be discovered, but Cloud Insights does not report on FC mapping, masking, or storage ports.

Terminology

Cloud Insights acquires the following inventory information from the Unity data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Disk	Disk
Storage Array	Storage
Processor	Storage Node
Storage Pool	Storage Pool
General iSCSI Block info, VMWare VMFS	Share
Replication Remote System	Synchronization
iSCSI Node	iSCSI Target Node

Vendor/Model Term	Cloud Insights Term
iSCSI Initiator	iSCSI Target Initiator

Note: These are common terminology mappings only and might not represent every case for this data source.

Configuration

Field	Description
Unity Storage	IP address or fully-qualified domain name of the Unity device
User Name	User name for the Unity device
Password	Password for the Unity device
Full Path to the Executable UEMCLI	Full path to the folder containing the <i>uemcli.exe</i> executable

Advanced configuration

Field	Description
Inventory Poll Interval (min)	Interval between inventory polls. The default is 40 minutes
Unity CLI Port	Port used for the Unity CLI
Performance poll interval (sec)	The default is 300.

Troubleshooting

Some things to try if you encounter problems with this data collector:

Inventory

Problem:	Try this:
"Failed to execute external utility" with error messages "Failed to find Unisphere executable uemcli"	<ul style="list-style-type: none"> * Verify correct IP address, username, and password * Confirm that Unisphere CLI is installed on the Cloud Insights Acquisition Unit * Confirm that Unisphere CLI installation directory is correct in the datasource configuration * Confirm that the IP of the VNXe is correct in the configuration of the datasource. From the Cloud Insights Acquisition Unit, open a CMD and change to the configured installation directory: \${INSTALLDIR}. Try to make a connection with the VNXe device by typing: <code>uemcli -d <Your IP> -u <Your ID> /sys/general show</code>

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Dell EMC VMAX and PowerMax Family of Devices data collector

Cloud Insights discovers EMC VMAX and PowerMax storage arrays by using Solutions Enabler symcli commands in conjunction with an existing Solutions Enabler server in your environment. The existing Solutions Enabler server has connectivity to the VMAX/PowerMax storage array through access to gatekeeper volumes.

Requirements

Before configuring this data collector, you should ensure that Cloud Insights has TCP connectivity to port 2707 on the existing Solutions Enabler server. Cloud Insights discovers all the Symmetrix arrays that are "Local" to this server, as seen in "symcfg list" output from that server.

- The EMC Solutions Enabler (CLI) with SMI-S provider application must be installed on the Acquisition Unit server and the version must match or be earlier than the version running on the Solutions Enabler Server.
- A properly configured {installdir}\EMC\SYMAP\config\netcnfg file is required. This file defines service names for Solutions Enabler servers, as well as the access method (SECURE / NOSECURE /ANY).
- If you require read/write latency at the storage node level, the SMI-S Provider must communicate with a running instance of the UNISPHERE for VMAX application.
- IP address of the managing Solutions Enabler server
- Administrator permissions on the Solutions Enabler (SE) Server
- Read-only user name and password to the SE software
- The UNISPHERE for VMAX application must be running and collecting statistics for the EMC VMAX and PowerMax storage arrays that are managed by the SMI-S Provider installation
- Access validation for performance: In a web browser on your Acquisition Unit, go to <https://<SMI-S Hostname or IP>:5989/ecomconfig> where "SMI-S Hostname or IP" is the IP address or hostname of your SMI-S server. This URL is for an administrative portal for the EMC SMI-S (aka "ECOM") service - you will receive a login popup.
- Permissions must be declared in the Solutions Enabler server's daemon configuration file, usually found here: `/var/sympapi/config/daemon_users`

Here is an example file with the proper cisys permissions.

```
root@cernciaukc101:/root
14:11:25 # tail /var/sympapi/config/daemon_users
#####
#####      Refer to the storrdfd(3) man page for additional details.
#####
#####      As noted above, only authorized users can perform stordaeamon
control
#####      operations (e.g., shutdown).
#####
# smith          storrdfd
cisys storapid <all>
```

Terminology

Cloud Insights acquires the following inventory information from the EMC VMAX/PowerMax data source. For each asset type acquired, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Disk	Disk
Disk Group	Disk Group
Storage	Array Storage
Director	Storage Node
Device Pool, Storage Resource Pool (SRP)	Storage Pool
Device TDev	Volume

Note: These are common terminology mappings only and might not represent every case for this data collector.

Configuration

Note: If SMI-S user authentication is not enabled, the default values in the Cloud Insights data collector are ignored.

Field	Description
Service Name	Service name as specified in <i>netcfg</i> file
Full path to CLI	Full path to the folder containing the Symmetrix CLI
SMI-S Host IP Address	IP address of the SMI-S host

Advanced Configuration

Field	Description
Inventory Poll Interval (min)	Interval between inventory polls. The default is 40 minutes.
Choose 'Exclude' or 'Include' to specify a list	Specify whether to include or exclude the array list below when collecting data.
Inventory Filter Device List	Comma-separated list of device IDs to include or exclude

Field	Description
Connection Caching	<p>Choose connection caching method:</p> <ul style="list-style-type: none"> * LOCAL means that the Cloud Insights Acquisition service is running on the Solutions Enabler server, which has Fibre Channel connectivity to the Symmetrix arrays you seek to discover, and has access to gatekeeper volumes. This might be seen in some Remote Acquisition Unit (RAU) configurations. * REMOTE_CACHED is the default and should be used in most cases. This uses the NETCNFG file settings to connect using IP to the Solutions Enabler server, which must have Fibre Channel connectivity to the Symmetrix arrays you seek to discover, and has access to Gatekeeper volumes. * In the event that REMOTE_CACHED options make CLI commands fail, use the REMOTE option. Keep in mind that it will slow down the acquisition process (possibly to hours or even days in extreme cases). The NETCNFG file settings are still used for an IP connection to the Solutions Enabler server that has Fibre Channel connectivity to the Symmetrix arrays being discovered. <p>Note: This setting does not change Cloud Insights behavior with respect to the arrays listed as REMOTE by the "symcfg list" output. Cloud Insights gathers data only on devices shown as LOCAL by this command.</p>
SMI-S Protocol	Protocol used to connect to the SMI-S provider. Also displays the default port used.
Override SMIS-Port	If blank, use the default port in the Connection Type field, otherwise enter the connection port to use
SMI-S User Name	User name for the SMI-S Provider Host
SMI-S Password	User name for the SMI-S Provider Host
Performance Polling Interval (sec)	Interval between performance polls (default 1000 seconds)
choose 'Exclude' or 'Include' to specify a list	Specify whether to include or exclude the array list below when collecting performance data
Performance Filter Device List	Comma-separated list of device IDs to include or exclude

Troubleshooting

Some things to try if you encounter problems with this data collector:

Problem:	Try this:
Error: The feature being requested is not currently licensed	Install the SYMAPI server license.
Error: No devices were found	Make sure Symmetrix devices are configured to be managed by the the Solutions Enabler server: - Run symcfg list -v to see the list of configured Symmetrix devices.
Error: A requested network service was not found in the service file	Make sure the Solutions Enabler Service Name is defined the netcnfg file for Solutions Enabler. This file is usually located under SYMAPI\config\ in the Solutions Enabler client installation.
Error: The remote client/server handshake failed	Check the most recent storsrvd.log* files on the Solutions Enabler host we are trying to discover.
Error: Common name in client certificate not valid	Edit the <i>hosts</i> file on the Solutions Enabler server so that the Acquisition Unit's hostname resolves to the IP address as reported in the storsrvd.log on the Solutions Enabler server.
Error: The function could not obtain memory	Make sure there is enough free memory available in the system to execute Solutions Enabler
Error: Solutions Enabler was unable to serve all data required.	Investigate the health status and load profile of Solutions Enabler
Error: • The "symcfg list -tdev" CLI command may return incorrect data when collected with Solutions Enabler 7.x from a Solutions Enabler server 8.x. • The "symcfg list -srp" CLI command may return incorrect data when collected with Solutions Enabler 8.1.0 or earlier from a Solutions Enabler server 8.3 or later.	Be sure you are using the same Solutions Enabler major release

Problem:	Try this:
<p>I'm seeing data collection errors with the message: "unknown code"</p>	<p>You may see this message if permissions are not declared in the Solutions Enabler server's daemon configuration file (see the Requirements above.) This assumes your SE client version matches your SE server version.</p> <p>This error may also occur if the <i>cisys</i> user (which executes Solutions Enabler commands) has not been configured with the necessary daemon permissions in the <code>/var/sympapi/config/daemon_users</code> configuration file.</p> <p>To fix this, edit the <code>/var/sympapi/config/daemon_users</code> file and make sure the <i>cisys</i> user has <code><all></code> permission specified for the <i>storapid</i> daemon.</p> <p>Example:</p> <pre>14:11:25 # tail /var/sympapi/config/daemon_users ... cisys storapid <all></pre>

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Dell EMC VNX Block Storage (NaviCLI) data collector

Cloud Insights uses the Dell EMC VNX Block Storage (NaviSec) data collector (formerly CLARiiON) to acquire inventory and performance data.

Terminology

Cloud Insights acquires the following inventory information from the EMC VNX Block Storage data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Disk	Disk
Storage	Storage
Storage Processor	Storage Node
This Pool, RAID Group	Storage Pool
LUN	Volume

Note: These are common terminology mappings only and might not represent every case for this data source.

Requirements

The following requirements must be met in order to collect data:

- An IP address of each VNX block storage processor
- Read-only Navisphere username and password to the VNX block storage arrays
- NaviSecCli must be installed on the Cloud Insights AU
- Access validation: Run NaviSecCLI from the Cloud Insights AU to each array using the username and password.
- Port requirements: 80, 443
- NaviSecCLI version should correspond with the newest FLARE code on your array
- For performance, statistics logging must be enabled.

NaviSphere command line interface syntax

`naviseccli.exe -h <IP address> -user <user> -password <password> -scope <scope, use 0 for global scope> -port <use 443 by default> command`

Configuration

Field	Description
VNX Block Storage IP Address	IP address or fully-qualified domain name of the VNX block storage
User Name	Name used to log into the VNX block storage device.
Password	Password used to log into the VNX block storage device.
CLI Path to naviseccli.exe	Full path to the folder containing the <i>naviseccli.exe</i> executable

Advanced Configuration

Field	Description
Inventory Poll Interval (min)	Interval between inventory polls. Default is 40 minutes.
Scope	The secure client scope. The default is Global.
Performance Poll Interval (sec)	Interval between performance polls. The default is 300 seconds.

Troubleshooting

Some things to try if you encounter problems with this data collector:

Inventory

Problem:	Try this:
Error: <ul style="list-style-type: none"> • Agent Not Running • Failed to find naviseccli • Failed to execute any command 	<ul style="list-style-type: none"> • Confirm that NaviSphere CLI is installed on the Cloud Insight Acquisition Unit • You have not selected the "Use secure client" option in the data collector configuration wizard and do not have a non-secure version of Navisphere CLI installed. • Confirm that NaviSphere CLI installation directory is correct in the data collector configuration • Confirm that the IP of the VNX block storage is correct in the data collector configuration: • From the Cloud Insights Acquisition Unit: <ul style="list-style-type: none"> - Open a CMD. - Change the directory to the configured installation directory - Try to make a connection with the VNX block storage device by typing “navicli -h {ip} getagent” (replace the {ip} with the actual IP)
Error: 4.29 emc235848 emc241018 getall Failed to parse host alias info	This is likely caused by a FLARE 29 corruption issue of the host initiator database on the array itself. See EMC knowledge base articles: emc235848, emc241018. You can also check https://now.netapp.com/Knowledgebase/solutionarea.asp?id=kb58128
Error: Unable to retrieve Meta LUNs. Error Executing java -jar navicli.jar	<ul style="list-style-type: none"> • Modify the data collector configuration to use the secure client (recommended) • Install navicli.jar in the CLI path to navicli.exe OR naviseccli.exe • Note: navicli.jar is deprecated as of EMC Navisphere version 6.26 • The navicli.jar may be available on http://powerlink.emc.com
Error: Storage Pools not reporting disks on Service Processor at configured IP address	Configure the data collector with both Service Processor IPs, separated by a comma
Error: Revision mismatch error	<ul style="list-style-type: none"> • This is usually caused by updating the firmware on the VNX block storage device, but not updating the installation of NaviCLI.exe. This also might be caused by having different devices with different firmwares, but only one CLI installed (with a different firmware version). • Verify that the device and the host are both running identical versions of the software: <ul style="list-style-type: none"> - From the Cloud Insights Acquisition Unit, open a command line window - Change the directory to the configured installation directory - Make a connection with the CLARiiON device by typing “navicli -h \${ip} getagent” - Look for the version number on the first couple of lines. Example: “Agent Rev: 6.16.2 (0.1)” - Look for and compare the version on the first line. Example: “Navisphere CLI Revision 6.07.00.04.07”

Problem:	Try this:
Error: Unsupported Configuration - No Fibre Channel Ports	The device is not configured with any Fibre Channel ports. Currently, only FC configurations are supported. Verify this version/firmware is supported.

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

DELL EMC VNX File (formerly Celerra Unified Storage System) data collector

This data collector acquires inventory information from the VNX File Storage System. For configuration, this data collector requires the IP address of the storage processors and a read-only user name and password.

Terminology

Cloud Insights acquires the following inventory information from the VNX File data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Celerra Network Server/Celerra Storage Pool	Storage Pool
File System	Internal Volume
Data Mover	Controller
File System mounted on a data mover	File Share
CIFS and NFS Exports	Share
Disk Volume	Backend LUN

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

You need the following to configure this data collector:

- The IP address of the storage processor
- Read-only user name and password
- SSH port 22

Configuration

Field	Description
VNX File IP Address	IP address or fully-qualified domain name of the VNX File device
User Name	Name used to log in to the VNX File device
Password	Password used to log in to the VNX File device

Advanced configuration

Field	Description
Inventory Poll Interval (minutes)	Interval between inventory polls. The default is 20 minutes.

Troubleshooting

Some things to try if you encounter problems with this data collector:

Inventory

Problem:	Try this:
Error: Unable to proceed while DART update in progress	Possible solution: Pause the data collector and wait for the DART upgrade to complete before attempting another acquisition request.

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Configuring the Dell EMC VNX Unified data collector

For configuration, the Dell EMC VNX Unified (SSH) data collector requires the IP address of the Control Station and a read-only username and password.

Terminology

Cloud Insights acquires the following inventory information from this data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Disk	Disk
Disk Folder	Disk Group
File system	Internal Volume
Storage	Storage
Storage Processor	Storage Node
Storage Pool, RAID Group	Storage Pool
LUN	Volume
Data Mover	Controller
File System mounted on a data mover	File Share
CIFS and NFS Exports	Share
Disk Volume	Backend LUN

Requirements

You need the following to configure the VNX (SSH) data collector:

- VNX IP address & Credentials to the Celerra Control Station.
- Read-only username and password.
- The data collector is able to run NaviCLI/NaviSecCLI commands against the backend array utilizing the DART OS NAS heads

Configuration

Field	Description
VNX IP Address	IP address or fully-qualified domain name of the VNX Control Station
User Name	User name for the VNX Control Station
Password	Password for the VNX Control Station

Advanced configuration

Field	Description
Inventory Poll Interval (min)	Interval between inventory polls. The default is 40 minutes.
Performance Poll Interval (sec).	Interval between performance polls. The default is 300 seconds.

Troubleshooting

Additional information on this Data Collector may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Configuring the EMC VPLEX data collector

This data collector acquires inventory and performance data from EMC VPLEX storage systems. For configuration, the data collector requires an IP address of the VPLEX server and an administrative level domain account.

Cloud Insights' performance collection from Vplex clusters requires that the performance archive service be operational, in order to populate the .CSV files and logs that Cloud Insights retrieves via SCP-based file copies. NetApp has observed that many Vplex firmware upgrade/management station updates will leave this functionality non-operational. Customers planning such upgrades may want to proactively ask Dell/EMC if their planned upgrade will leave this functionality inoperable, and if so, how can they re-enable it to minimize gaps in performance visibility? Cloud Insight's Vplex performance code will assess on each poll whether all the expected files exist, and if they are being properly updated; if they are missing or stale, Cloud Insights will log performance collection failures.



Terminology

Cloud Insights acquires the following inventory information from the VPLEX data collector. For each asset type acquired, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Cluster	Storage
Engine	Storage Node
Device, System Extent	Backend Storage Pool
Virtual Volume	Volume
Front-End Port, Back-End Port	Port
Distributed Device	Storage Synchronization
Storage View	Volume Map, Volume Mask
Storage Volume	Backend LUN
ITLs	Backend Path

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

- An IP address of the VPLEX Management Console
- Administrative level domain account for the VPLEX server
- Port 443 (HTTPS). Requires outbound connectivity to TCP port 443 on the VPLEX management station.
- For performance, read-only username and password for ssh/scp access.
- For performance, port 22 is required.

Configuration

Field	Description
IP address of VPLEX Management Console	IP address or fully-qualified domain name of the VPLEX Management Console
User Name	User name for VPLEX CLI
Password	Password used for VPLEX CLI
Performance Remote IP Address	Performance Remote IP address of the VPLEX Management Console
Performance Remote User Name	Performance Remote user name of VPLEX Management Console
Performance Remote Password	Performance Remote Password of VPLEX Management Console

Advanced configuration

Field	Description
Communication Port	Port used for VPLEX CLI. The default is 443.
Inventory Poll Interval (min)	The default is 20 minutes.
Number of connection retries	The default is 3.
Performance Poll Interval (sec)	Interval between performance polls. The default is 600 seconds.
Number of Retries	The default is 2.

Troubleshooting

Some things to try if you encounter problems with this data collector:

Inventory

Problem:	Try this:
Error: User authentication failed.	Make sure your credentials for this device are correct.

Performance

Problem:	Try this:
Error: VPLEX performance for version below 5.3 is not supported.	Upgrade VPLEX to 5.3 or above
Error: No enough data collected.	<ul style="list-style-type: none">Check collection timestamp in log file and modify polling interval accordinglyWait for longer time
Error: Perpetual Log files not being updated.	Please contact EMC support to enable updating the perpetual log files
Error: Performance polling interval is too big.	Check collection timestamp in log file \${logfile} and modify polling interval accordingly
Error: Performance Remote IP address of VPLEX Management Console is not configured.	Edit the data source to set Performance Remote IP address of VPLEX Management Console.
Error: No performance data reported from director	<ul style="list-style-type: none">Check that the system performance monitors are running correctlyPlease contact EMC support to enable updating the system performance monitor log files

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Dell EMC XtremIO data collector

The EMC XtremIO data collector acquires inventory and performance data from the EMC XtremIO storage system.

Requirements

To configure the EMC XtremlO (HTTP) data collector, you must have:

- The XtremlO Management Server (XMS) Host address
- An account with administrator privileges
- Access to port 443 (HTTPS)

Terminology

Cloud Insights acquires the following inventory information from the EMC XtremlO data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Disk (SSD)	Disk
Cluster	Storage
Controller	Storage Node
Volume	Volume
LUN Map	Volume Map
Target FC Initiator	Volume Mask

Note: These are common terminology mappings only and might not represent every case for this data source.

Requirements

- The XtremlO Management Server (XMS) Host IP address
- Administrator user name and password for the XtremlO

Configuration

Field	Description
XMS Host	IP address or fully-qualified domain name of the XtremlO Management Server
User name	User name for the XtremlO Management Server
Password	Password for the XtremlO Management Server

Advanced configuration

Field	Description
TCP port	TCP Port used to connect to XTremlO Management Server. The default is 443.
Inventory poll interval (min)	Interval between inventory polls. The default is 60 minutes.

Field	Description
Performance poll interval (sec)	Interval between performance polls. The default is 300 seconds.

Troubleshooting

Additional information on this Data Collector may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Fujitsu Eternus data collector

The Fujitsu Eternus data collector acquires inventory data using administration-level access to the storage system.

Terminology

Cloud Insights acquires the following inventory information from the Fujitsu Eternus storage. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Disk	Disk
Storage	Storage
Thin Pool, Flexible Tier Pool, Raid Group	Storage Pool
Standard Volume, Snap Data Volume (SDV), Snap Data Pool Volume (SDPV), Thin Provisioning Volume (TPV), Flexible Tier Volume (FTV), Wide Striping Volume (WSV)	Volume
Channel adapter	Controller

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

The following are required to configure this data collector:

- An IP address of the Eternus storage, which cannot be comma delimited
- SSH Administration-level user name and password
- Port 22
- Ensure that the page scroll is disabled (clienv-show-more-scroll disable)

Configuration

Field	Description
IP Address of Eternus Storage	IP address of the Eternus storage
User Name	User name for Eternus storage
Password	Password for the Eternus storage

Advanced configuration

Field	Description
Inventory Poll Interval (min)	The default is 20 minutes.

Troubleshooting

Some things to try if you encounter problems with this data collector:

Inventory

Problem:	Try this:
"Error retrieving data" with error messages "Error Finding Prompt CLI" or "Error finding prompt at the end of shell results"	Likely caused by: Storage system has page scrolling enabled. Possible solution: * Try to disable page scrolling by running the following command: <code>set clienv-show-more -scroll disable</code>
"Connecting error" with error messages "Failed to instantiate an SSH connection to storage" or "Failed to instantiate a connection to VirtualCenter"	Likely causes: * Incorrect credentials. * Incorrect IP address. * Network problem. * Storage may be down or unresponsive. Possible solutions: * Verify credentials and IP address entered. * Try to communicate with storage using SSH Client.

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

NetApp Google Compute data collector

This data collector supports inventory and performance collection from Google Compute cloud platform configurations. This collector will seek to discover all the Compute resources within all the Projects within one Google organization. If you have multiple Google organizations you want to discover with Cloud Insights, you will want to deploy one Cloud Insights collector per organization.

Configuration

Field	Description
Organization ID	The organization ID you want to discover with this collector. This field is required if your service account is able to see more than one organization
Choose 'Exclude' or 'Include' to filter GCP Projects by IDs	If you want to limit what projects' resources are brought into Cloud Insights.
Project IDs	The list of Project IDs that you want to filter in, or out from discovery, depending on the value of the "Choose 'Exclude'"...." value. The default list is empty
Client ID	Client ID for the Google Cloud Platform configuration
Copy and paste the contents of your Google Credential File here	Copy your Google credentials for the Cloud Platform account to this field

Advanced configuration

Field	Description
Inventory Poll Interval (min)	Default is 60 minutes
Choose 'Exclude' or 'Include' to Apply to Filter VMs by Labels	Specify whether to include or exclude VM's by Labels when collecting data. If 'Include' is selected, the Label Key field can not be empty.
Label Keys and Values on which to Filter VMs	Click + Filter Label to choose which VMs (and associated disks) to include/exclude by filtering for keys and values that match keys and values of labels on the VM. Label Key is required, Label Value is optional. When Label Value is empty, the VM is filtered as long as it matches the Label Key.
Performance Poll Interval (sec)	Default is 1800 seconds

Troubleshooting

Additional information on this Data Collector may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

HP Enterprise

HP Enterprise Alletra 9000 / Primera Storage data collector

Cloud Insights uses the HP Enterprise Alletra 9000 / HP Enterprise Primera (previously 3PAR) data collector to discover inventory and performance.

Terminology

Cloud Insights acquires the following inventory information from this data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Field	Description
Physical Disk	Disk
Storage System	Storage
Controller Node	Storage Node
Common Provisioning Group	Storage Pool
Virtual Volume	Volume

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

The following are required to configure this data collector:

- IP address or FQDN of the InServ cluster
- For inventory, read-only user name and password to the StoreServ Server
- For performance, read-write user name and password to the StoreServ Server
- Port requirements: 22 (inventory collection), 5988 or 5989 (performance collection) [Note: Performance is supported for StoreServ OS 3.x+]
- For performance collection confirm that SMI-S is enabled by logging into the array via SSH.

Configuration

Field	Description
Storage IP address	Storage IP address or fully-qualified domain name of the StoreServ cluster
User Name	User name for the StoreServ Server
Password	Password used for the StoreServ Server
SMI-S User Name	User name for the SMI-S Provider Host
SMI-S Password	Password used for the SMI-S Provider Host

Advanced configuration

Field	Description
Inventory Poll Interval (min)	Interval between inventory polls. The default is 40 minutes.
SMI-S Connectivity	Protocol used to connect to the SMI-S provider
Override SMI-S Default Port	If blank, use the default port from SMI-S Connectivity, otherwise enter the connection port to use
Performance Poll Interval (sec)	Interval between performance polls. The default is 300 seconds.

Troubleshooting

Some things to try if you encounter problems with this data collector:

Inventory

Problem:	Try this:
"showsys" command doesn't return any result.	Run "showsys" and "showversion -a" from the command line and check if the version is supported by the array.

Performance

Problem:	Try this:
Failed to connect or login. Provider initialization failed.	An all-numeric array name can cause problems with SMI-S server. Try changing the array name.
SMI-S user configured does not have any domain	Grant appropriate domain privileges to the configured SMI-S user
Cloud Insights states that it cannot connect/login to SMI-S service.	Confirm there is no firewall between the CI AU and the array that would block the CI AU from making TCP connections to 5988 or 5989. Once that is done, and if you have confirmed there is no firewall, you should SSH to the array, and use the "showcim" command to confirm. Verify that: <ul style="list-style-type: none">* Service is enabled* HTTPS is enabled* HTTPS port should be 5989 If those all are so, you can try to "stopcim" and then a "startcim" to restart the CIM (i.e. SMI-S service).

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

HP Enterprise Command View data collector

The HP Enterprise Command View Advanced Edition data collector supports discovering XP and P9500 arrays via Command View Advanced Edition (CVAE) server. Cloud Insights communicates with CVAE using the standard Command View API to collect inventory and performance data.

Terminology

Cloud Insights acquires the following inventory information from the HP Enterprise Command View data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
PDEV	Disk
Journal Pool	Disk Group
Storage Array	Storage
Port Controller	Storage Node
Array Group, DP Pool	Storage Pool
Logical Unit, LDEV	Volume

Note: These are common terminology mappings only and might not represent every case for this data collector.

Inventory requirements

You must have the following in order to collect inventory data:

- IP address of the CVAE server
- Read-only user name and password for the CVAE software and peer privileges
- Port requirement: 2001

Performance requirements

The following requirements must be met in order to collect performance data:

- HDS USP, USP V, and VSP performance
 - Performance Monitor must be licensed.
 - Monitoring switch must be enabled.
 - The Export Tool (Export.exe) must be copied to the Cloud Insights AU and extracted to a location. On CI Linux AUs, ensure "cisys" has read and execute permissions.
 - The Export Tool version must match the microcode version of the target array.
- AMS performance:
 - Performance Monitor must be licensed.
 - The Storage Navigator Modular 2 (SNM2) CLI utility be installed on the Cloud Insights AU.
- Network requirements
 - The Export Tools are Java based, and use RMI to speak to the array. These tools may not be firewall-friendly as they may dynamically negotiate source and destination TCP ports on each invocation. Also, different model array's Export Tools may behave differently across the network - consult HPE for your model's requirements

Configuration

Field	Description
Command View Server	IP address or fully-qualified domain name of the Command View server

Field	Description
User Name	User name for the Command View server.
Password	Password used for the Command View server.
Devices - VSP G1000 (R800), VSP (R700), HUS VM (HM700) and USP storages	Device list for VSP G1000 (R800), VSP (R700), HUS VM (HM700) and USP storages. Each storage requires: * Array's IP: IP address of the storage * User Name: User name for the storage * Password: Password for the storage * Folder Containing Export Utility JAR Files
SNM2Devices - WMS/SMS/AMS Storages	Device list for WMS/SMS/AMS storages. Each storage requires: * Array's IP: IP address of the storage * Storage Navigator CLI Path: SNM2 CLI path * Account Authentication Valid: Select to choose valid account authentication * User Name: User name for the storage * Password: Password for the storage
Choose Tuning Manager for Performance	Override other performance options
Tuning Manager Host	IP address or fully-qualified domain name of tuning manager
Tuning Manager Port	Port used for Tuning Manager
Tuning Manager Username	User name for Tuning Manager
Tuning Manager Password	Password for Tuning Manager

Note: In HDS USP, USP V, and VSP, any disk can belong to more than one array group.

Advanced configuration

Field	Description
Command View Server Port	Port used for the Command View Server
HTTPs Enabled	Select to enable HTTPs
Inventory Poll Interval (min)	Interval between inventory polls. The default is 40.
Choose 'Exclude' or 'Include' to specify a list	Specify whether to include or exclude the array list below when collecting data.
Exclude or Include Devices	Comma-separated list of device ID's or array names to include or exclude
Query Host Manager	Select to query host manager
Performance Polling Interval (sec)	Interval between performance polls. The default is 300.

Troubleshooting

Some things to try if you encounter problems with this data collector:

Inventory

Problem:	Try this:
Error: User does not have enough permission	Use a different user account that has more privilege or increase the privilege of user account configured in the data collector
Error: Storages list is empty. Either devices are not configured or the user does not have enough permission	* Use DeviceManager to check if the devices are configured. * Use a different user account that has more privilege, or increase the privilege of the user account
Error: HDS storage array was not refreshed for some days	Investigate why this array is not being refreshed in HP CommandView AE.

Performance

Problem:	Try this:
Error: * Error executing export utility * Error executing external command	* Confirm that Export Utility is installed on the Cloud Insights Acquisition Unit * Confirm that Export Utility location is correct in the data collector configuration * Confirm that the IP of the USP/R600 array is correct in the configuration of the data collector * Confirm that the User name and password are correct in the configuration of the data collector * Confirm that Export Utility version is compatible with storage array micro code version * From the Cloud Insights Acquisition Unit, open a CMD prompt and do the following: - Change the directory to the configured installation directory - Try to make a connection with the configured storage array by executing batch file runWin.bat
Error: Export tool login failed for target IP	* Confirm that username/password is correct * Create a user ID mainly for this HDS data collector * Confirm that no other data collectors are configured to acquire this array
Error: Export tools logged "Unable to get time range for monitoring".	* Confirm performance monitoring is enabled on the array. * Try invoking the export tools outside of Cloud Insights to confirm the problem lies outside of Cloud Insights.

Problem:	Try this:
Error: * Configuration error: Storage Array not supported by Export Utility * Configuration error: Storage Array not supported by Storage Navigator Modular CLI	* Configure only supported storage arrays. * Use "Filter Device List" to exclude unsupported storage arrays.
Error: * Error executing external command * Configuration error: Storage Array not reported by Inventory * Configuration error: export folder does not contain jar files	* Check Export utility location. * Check if Storage Array in question is configured in Command View server * Set Performance poll interval as multiple of 60 seconds.
Error: * Error Storage navigator CLI * Error executing auperform command * Error executing external command	* Confirm that Storage Navigator Modular CLI is installed on the Cloud Insights Acquisition Unit * Confirm that Storage Navigator Modular CLI location is correct in the data collector configuration * Confirm that the IP of the WMS/SMS/SMS array is correct in the configuration of the data collector * Confirm that Storage Navigator Modular CLI version is compatible with micro code version of storage array configured in the data collector * From the Cloud Insights Acquisition Unit, open a CMD prompt and do the following: - Change the directory to the configured installation directory - Try to make a connection with the configured storage array by executing following command "auunitref.exe"
Error: Configuration error: Storage Array not reported by Inventory	Check if Storage Array in question is configured in Command View server
Error: * No Array is registered with the Storage Navigator Modular 2 CLI * Array is not registered with the Storage Navigator Modular 2 CLI * Configuration error: Storage Array not registered with StorageNavigator Modular CLI	* Open Command prompt and change directory to the configured path * Run the command "set=STONAVM_HOME=." * Run the command "auunitref" * Confirm that the command output contains details of the array with IP * If the output does not contain the array details then register the array with Storage Navigator CLI: - Open Command prompt and change directory to the configured path - Run the command "set=STONAVM_HOME=." - Run command "auunitaddauto -ip \${ip} ". Replace \${ip} with real IP

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

HPE Alletra 6000 data collector

The HP Enterprise Alletra 6000 (previously Nimble) data collector supports inventory and performance data for Alletra 6000 storage arrays.

Terminology

Cloud Insights acquires the following inventory information from this collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Array	Storage
Disk	Disk
Volume	Volume
Pool	Storage Pool
Initiator	Storage Host Alias
Controller	Storage Node
Fibre Channel Interface	Controller

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

You must have the following in order to collect inventory and configuration data from the storage array:

- The array must be installed and configured, and reachable from the client through its fully qualified domain name (FQDN) or array management IP address.
- The array must be running NimbleOS 2.3.x or later.
- You must have a valid user name and password to the array with at least "Operator" level role. The "Guest" role does not have sufficient access to understand initiator configurations.
- Port 5392 must be open on the array.

You must have the following in order to collect performance data from the storage array:

- The array must be running NimbleOS 4.0.0 or later
- The array must have volumes configured. The only performance API NimbleOS has is for volumes, and any statistics Cloud Insights reports are derived from the statistics on volumes

Configuration

Field	Description
Array Management IP Address	Fully qualified domain name (FQDN) or array management IP address.
User Name	User name for the array
Password	Password for the array

Advanced configuration

Field	Description
Port	Port used by Nimble REST API. The default is 5392.
Inventory Poll Interval (min)	Interval between inventory polls. The default is 60 minutes.

Note: The default performance poll interval is 300 seconds and can not be changed. This is the only interval supported by HPE Alletra 6000.

Hitachi Data Systems

Hitachi Vantara Command Suite data collector

The Hitachi Vantara Command Suite data collector supports the HiCommand Device Manager server. Cloud Insights communicates with the HiCommand Device Manager server using the standard HiCommand API.

Terminology

Cloud Insights acquires the following inventory information from the Hitachi Vantara Command Suite data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
PDEV	Disk
Journal Pool	Disk Group
Storage Array	Storage
Port Controller	Storage Node
Array Group, HDS Pool	Storage Pool
Logical Unit, LDEV	Volume

Note: These are common terminology mappings only and might not represent every case for this data collector.

Storage

The following terms apply to objects or references that you might find on HDS storage asset landing pages. Many of these terms apply to other data collectors as well.

- Name – comes directly from HDS HiCommand Device Manager’s “name” attribute via the GetStorageArray XML API call
- Model - comes directly from HDS HiCommand Device Manager’s “arrayType” attribute via the GetStorageArray XML API call
- Vendor – HDS
- Family - comes directly from HDS HiCommand Device Manager’s “arrayFamily” attribute via the GetStorageArray XML API call

- IP – this is the management IP address of the array, not an exhaustive list of all IP addresses on the array
- Raw Capacity – a base2 value representing the sum of the total capacity of all disks in this system, regardless of disk role.

Storage Pool

The following terms apply to objects or references that you might find on HDS storage pool asset landing pages. Many of these terms apply to other data collectors as well.

- Type: The value here will be one of:
 - RESERVED – if this pool is dedicated for purposes other than data volumes, i.e, journaling, snapshots
 - Thin Provisioning – if this is a HDP pool
 - Raid Group – you will not likely see these for a few reasons:

Cloud Insights takes a strong stance to avoid double counting capacity at all costs. On HDS, one typically needs to build Raid Groups from disks, create pool volumes on those Raid Groups, and construct pools (often HDP, but could be special purpose) from those pool volumes. If Cloud Insights reported both the underlying Raid Groups as is, as well as the Pools, the sum of their raw capacity would vastly exceed the sum of the disks.

Instead, Cloud Insights' HDS Command Suite data collector arbitrarily shrinks the size of Raid Groups by the capacity of pool volumes. This may result in Cloud Insights not reporting the Raid Group at all. Additionally, any resulting Raid Groups are flagged in a way such that they are not visible in the Cloud Insights WebUI, but they do flow into the Cloud Insights Data Warehouse (DWH). The purpose of these decisions is to avoid UI clutter for things that most users do not care about – if your HDS array has Raid Groups with 50MB free, you probably cannot use that free space for any meaningful outcome.

- Node - N/A, as HDS pools are not tied to any one specific node
- Redundancy - the RAID level of the pool. Possibly multiple values for a HDP pool comprised of multiple RAID types
- Capacity % - the percent used of the pool for data usage, with the used GB and total logical GB size of the pool
- Over-committed Capacity - a derived value, stating “the logical capacity of this pool is oversubscribed by this percentage by virtue of the sum of the logical volumes exceeding the logical capacity of the pool by this percentage”
- Snapshot - shows the capacity reserved for snapshot usage on this pool

Storage Node

The following terms apply to objects or references that you might find on HDS storage node asset landing pages. Many of these terms apply to other data collectors as well.

- Name – The name of the Front-end director (FED) or Channel Adapter on monolithic arrays, or the name of the controller on a modular array. A given HDS array will have 2 or more Storage Nodes
- Volumes – The Volume table will show any volume mapped to any port owned by this storage node

Inventory Requirements

You must have the following in order to collect inventory data:

- IP address of the HiCommand Device Manager server

- Read-only user name and password for the HiCommand Device Manager software and peer privileges
- Port requirements: 2001 (http) or 2443 (https)
- Log into HiCommand Device Manager software using username and password
- Verify access to HiCommand Device Manager http://<HiCommand_Device_Manager_IP>:2001/service/StorageManager

Performance requirements

The following requirements must be met in order to collect performance data:

- HDS USP, USP V, and VSP performance
 - Performance Monitor must be licensed.
 - Monitoring switch must be enabled.
 - The Export Tool (Export.exe) must be copied to the Cloud Insights AU.
 - The Export Tool version must match the microcode version of the target array.
- AMS performance:
 - NetApp strongly recommends creating a dedicated service account on AMS arrays for Cloud Insights to use to retrieve performance data. Storage Navigator only allows a user account one concurrent login to the array. Having Cloud Insights use the same user account as management scripts or HiCommand may result in Cloud Insights, management scripts, or HiCommand being unable to communicate to the array due to the one concurrent user account login limit
 - Performance Monitor must be licensed.
 - The Storage Navigator Modular 2 (SNM2) CLI utility needs to be installed on the Cloud Insights AU.

Configuration

Field	Description
HiCommand Server	IP address or fully-qualified domain name of the HiCommand Device Manager server
User Name	User name for the HiCommand Device Manager server.
Password	Password used for the HiCommand Device Manager server.
Devices - VSP G1000 (R800), VSP (R700), HUS VM (HM700) and USP storages	<p>Device list for VSP G1000 (R800), VSP (R700), HUS VM (HM700) and USP storages. Each storage requires:</p> <ul style="list-style-type: none"> * Array's IP: IP address of the storage * User Name: User name for the storage * Password: Password for the storage * Folder Containing Export Utility JAR Files

Field	Description
SNM2Devices - WMS/SMS/AMS Storages	Device list for WMS/SMS/AMS storages. Each storage requires: * Array's IP: IP address of the storage * Storage Navigator CLI Path: SNM2 CLI path * Account Authentication Valid: Select to choose valid account authentication * User Name: User name for the storage * Password: Password for the storage
Choose Tuning Manager for Performance	Override other performance options
Tuning Manager Host	IP address or fully-qualified domain name of tuning manager
Override Tuning Manager Port	If blank, use the default port in the Choose Tuning Manager for Performance field, otherwise enter the port to use
Tuning Manager Username	User name for Tuning Manager
Tuning Manager Password	Password for Tuning Manager

Note: In HDS USP, USP V, and VSP, any disk can belong to more than one array group.

Advanced configuration

Field	Description
Connection Type	HTTPS or HTTP, also displays the default port
HiCommand Server Port	Port used for the HiCommand Device Manager
Inventory Poll Interval (min)	Interval between inventory polls. The default is 40.
Choose 'Exclude' or 'Include' to specify a list	Specify whether to include or exclude the array list below when collecting data.
Filter device List	Comma-separated list of device serial numbers to include or exclude
Performance Poll Interval (sec)	Interval between performance polls. The default is 300.
Export timeout in seconds	Export utility timeout. The default is 300.

Troubleshooting

Some things to try if you encounter problems with this data collector:

Inventory

Problem:	Try this:
Error: User does not have enough permission	Use a different user account that has more privilege or increase the privilege of user account configured in the data collector
Error: Storages list is empty. Either devices are not configured or the user does not have enough permission	<ul style="list-style-type: none"> * Use DeviceManager to check if the devices are configured. * Use a different user account that has more privilege, or increase the privilege of the user account
Error: HDS storage array was not refreshed for some days	Investigate why this array is not being refreshed in HDS HiCommand.

Performance

Problem:	Try this:
Error: * Error executing export utility * Error executing external command	<ul style="list-style-type: none"> * Confirm that Export Utility is installed on the Cloud Insights Acquisition Unit * Confirm that Export Utility location is correct in the data collector configuration * Confirm that the IP of the USP/R600 array is correct in the configuration of the data collector * Confirm that the User name and password are correct in the configuration of the data collector * Confirm that Export Utility version is compatible with storage array micro code version * From the Cloud Insights Acquisition Unit, open a CMD prompt and do the following: <ul style="list-style-type: none"> - Change the directory to the configured installation directory - Try to make a connection with the configured storage array by executing batch file runWin.bat
Error: Export tool login failed for target IP	<ul style="list-style-type: none"> * Confirm that username/password is correct * Create a user ID mainly for this HDS data collector * Confirm that no other data collectors are configured to acquire this array
Error: Export tools logged "Unable to get time range for monitoring".	<ul style="list-style-type: none"> * Confirm performance monitoring is enabled on the array. * Try invoking the export tools outside of Cloud Insights to confirm the problem lies outside of Cloud Insights.
Error: * Configuration error: Storage Array not supported by Export Utility * Configuration error: Storage Array not supported by Storage Navigator Modular CLI	<ul style="list-style-type: none"> * Configure only supported storage arrays. * Use "Filter Device List" to exclude unsupported storage arrays.

Problem:	Try this:
Error: * Error executing external command * Configuration error: Storage Array not reported by Inventory * Configuration error: export folder does not contain jar files	* Check Export utility location. * Check if Storage Array in question is configured in HiCommand server * Set Performance poll interval as multiple of 60 seconds.
Error: * Error Storage navigator CLI * Error executing auperform command * Error executing external command	* Confirm that Storage Navigator Modular CLI is installed on the Cloud Insights Acquisition Unit * Confirm that Storage Navigator Modular CLI location is correct in the data collector configuration * Confirm that the IP of the WMS/SMS/SMS array is correct in the configuration of the data collector * Confirm that Storage Navigator Modular CLI version is compatible with micro code version of storage array configured in the data collector * From the Cloud Insights Acquisition Unit, open a CMD prompt and do the following: - Change the directory to the configured installation directory - Try to make a connection with the configured storage array by executing following command "auunitref.exe"
Error: Configuration error: Storage Array not reported by Inventory	Check if Storage Array in question is configured in HiCommand server
Error: * No Array is registered with the Storage Navigator Modular 2 CLI * Array is not registered with the Storage Navigator Modular 2 CLI * Configuration error: Storage Array not registered with StorageNavigator Modular CLI	* Open Command prompt and change directory to the configured path * Run the command "set=STONAVM_HOME=." * Run the command "auunitref" * Confirm that the command output contains details of the array with IP * If the output does not contain the array details then register the array with Storage Navigator CLI: - Open Command prompt and change directory to the configured path - Run the command "set=STONAVM_HOME=." - Run command "auunitaddauto -ip \${ip} ". Replace \${ip} with real IP

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Configuring the Hitachi Vantara NAS data collector

The Hitachi Vantara NAS data collector is an inventory and configuration data collector that supports discovery of HDS NAS clusters. Cloud Insights supports discovering NFS and CIFS shares, file systems (Internal Volumes), and spans (Storage Pools).

Terminology

Cloud Insights acquires the following inventory information from the HNAS data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or

troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Tier	Disk Group
Cluster	Storage
Node	Storage Node
Span	Storage Pool
System Drive	Backend Lun
Files System	Internal Volume

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

- Device IP address
- Port 22, SSH protocol
- Username and password - privilege level: Supervisor
- Note: This data collector is SSH based, so the AU that hosts it must be able to initiate SSH sessions to TCP 22 on the HNAS itself, or the Systems Management Unit (SMU) that the cluster is connected to.

Configuration

Field	Description
HNAS Host	IP address or fully-qualified domain name of HNAS Management Host
User Name	User name for HNAS CLI
Password	Password used for HNAS CLI

Advanced configuration

Field	Description
Inventory Poll Interval (min)	Interval between inventory polls. The default is 30 minutes.

Troubleshooting

Some things to try if you encounter problems with this data collector:

Inventory

Problem:	Try this:
"Error connecting" with error messages "Error setting up shell channel:" or "Error opening shell channel"	Likely caused by network connectivity issues or SSH is misconfigured. Confirm connection with alternate SSH client
"Timeout" or "Error retrieving data" with error messages "Command: XXX has timed out."	* Try the command with alternate SSH client * Increase timeout
"Error connecting " or "Invalid login credentials" with error messages "Could not communicate with the device:"	* Check IP address * Check user name and password * Confirm connection with alternate SSH client

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Hitachi Ops Center data collector

This data collector uses Hitachi Ops Center's integrated suite of applications to access inventory and performance data of multiple storage devices. For inventory and capacity discovery, your Ops Center installation must include both the "Common Services" and "Administrator" components. For performance collection, you must additionally have "Analyzer" deployed.

Terminology

Cloud Insights acquires the following inventory information from this data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Storage Systems	Storage
Volume	Volume
Parity Groups	Storage Pool(RAID), Disk Groups
Disk	Disk
Storage Pool	Storage Pool(Thin, SNAP)
External Parity Groups	Storage Pool(Backend), Disk Groups
Port	Storage Node → Controller Node → Port
Host Groups	Volume Mapping and Masking
Volume Pairs	Storage Synchronization

Note: These are common terminology mappings only and might not represent every case for this data collector.

Inventory Requirements

You must have the following in order to collect inventory data:

- IP address or hostname of the Ops Center server hosting the "Common Services" component
- Root/sysadmin user account and password that exist on all servers hosting Ops Center components. HDS did not implement REST API support for usage by LDAP/SSO users until Ops Center 10.8+

Performance requirements

The following requirements must be met in order to collect performance data:

The HDS Ops Center "Analyzer" module must be installed
Storage arrays must be feeding the Ops Center "Analyzer" module

Configuration

Field	Description
Hitachi Ops Center IP Address	IP address or fully-qualified domain name of the Ops Center server hosting the "Common Services" component
User Name	User name for the Ops Center server.
Password	Password used for the Ops Center server.

Advanced configuration

Field	Description
Connection Type	HTTPS (port 443) is the default
Override TCP Port	Specify the port to use if not the default
Inventory Poll Interval (min)	Interval between inventory polls. The default is 40.
Choose 'Exclude' or 'Include' to specify a list	Specify whether to include or exclude the array list below when collecting data.
Filter device List	Comma-separated list of device serial numbers to include or exclude
Performance Poll Interval (sec)	Interval between performance polls. The default is 300.

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Infinidat InfiniBox data collector

The Infinidat InfiniBox (HTTP) data collector is used to collect inventory information from the Infinidat InfiniBox storage system.

Terminology

Cloud Insights acquires the following inventory information from the Infinidat InfiniBox data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Storage Pool	Storage Pool
Node	Controller
Filesystem	Internal Volume
Filesystem	File Share
Filesystem Exports	Share

Requirements

The following are requirements when configuring this data collector.

- IP address or FQDN of InfiniBox management Node
- Admin userid and password
- Port 443 via REST API

Configuration

Field	Description
InfiniBox Host	IP address or fully-qualified domain name of the InfiniBox Management Node
User Name	User name for InfiniBox Management Node
Password	Password for the InfiniBox Management Node

Advanced configuration

Field	Description
TCP Port	TCP Port used to connect to InfiniBox Server. The default is 443.
Inventory Poll Interval	Interval between inventory polls. The default is 60 minutes.

Troubleshooting

Additional information on this Data Collector may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Huawei OceanStor data collector

Cloud Insights uses the Huawei OceanStor (REST/HTTPS) data collector to discover inventory and performance for Huawei OceanStor and OceanStor Dorado storage.

Terminology

Cloud Insights acquires the following inventory and performance information from the Huawei OceanStor. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Storage Pool	Storage Pool
File System	Internal Volume
Controller	Storage Node
FC Port (Mapped)	Volume Map
Host FC Initiator (Mapped)	Volume Mask
NFS/CIFS Share	Share
iSCSI Link Target	iSCSI Target Node
iSCSI Link Initiator	iSCSI Initiator Node
Disk	Disk
LUN	Volume

Requirements

The following requirements are required to configure this data collector:

- Device IP address
- Credentials to access OceanStor device manager
- Port 8088 must be available

Configuration

Field	Description
OceanStor Host IP Address	IP address or fully-qualified domain name of the OceanStor Device Manager
User Name	Name used to log into the OceanStor Device Manager
Password	Password used to log into the OceanStor Device Manager

Advanced Configuration

Field	Description
TCP Port	TCP Port used to connect to OceanStor Device Manager. The default is 8088.
Inventory Poll Interval (min)	Interval between inventory polls. The default is 60 minutes.

Field	Description
Performance poll interval (sec).	The default is 300 seconds.

Troubleshooting

Additional information on this Data Collector may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

IBM

IBM Cleversafe data collector

Cloud Insights uses this data collector to discover inventory and performance data for IBM Cleversafe storage systems.



IBM Cleversafe is metered at a different Raw TB to Managed Unit rate. Every 40 TB of unformatted IBM Cleversafe capacity is charged as 1 [Managed Unit \(MU\)](#).

Terminology

Cloud Insights acquires the following inventory information from the IBM Cleversafe data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Storage Pool	Storage Pool
Container	Internal Volume
Container	File Share
NFS Share	Share

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

- The external data services IP address for the cluster
- Administrator user name and password
- Port 9440

Configuration

Field	Description
Manager IP or host name	IP address or hostname of management node
User name	Username for the user account with super user or system administrator role

Field	Description
Password	Password for the user account with super user or system administrator role

Advanced configuration

Field	Description
Inventory poll interval (min)	Interval between inventory polls.
HTTP Connection Timeout (sec)	HTTP timeout in seconds.

Troubleshooting

Additional information on this Data Collector may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

IBM CS data collector

Cloud Insights uses this data collector to discover inventory and performance data for IBM CS storage systems.

Terminology

Cloud Insights acquires the following inventory information from the IBM CS data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Storage Pool	Storage Pool
Container	Internal Volume
Container	File Share
NFS Share	Share

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

- The external data services IP address for the cluster
- Administrator user name and password
- Port 9440

Configuration

Field	Description
Prism External IP Address	The external data services IP address for the cluster

Field	Description
User name	User name for the Admin account
Password	Password for the Admin account

Advanced configuration

Field	Description
TCP port	TCP Port used to connect to the IBM CS array. The default is 9440.
Inventory poll interval (min)	Interval between inventory polls. The default is 60 minutes.
Performance poll interval(sec)	Interval between performance polls. The default is 300 seconds.

Troubleshooting

Additional information on this Data Collector may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

IBM System Storage DS8000 Series data collector

The IBM DS (CLI) data collector supports inventory and performance data acquisition for DS6xxx and DS8xxx devices.

DS3xxx, DS4xxx, and DS5xxx devices are supported by the [NetApp E-Series data collector](#). You should refer to the Cloud Insights support matrix for supported models and firmware versions.

Terminology

Cloud Insights acquires the following inventory information from the IBM DS data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Disk Drive Module	Disk
Storage Image	Storage
Extent Pool	Storage Node
Fixed Block Volume	Volume
Host FC Initiator (Mapped)	Volume Mask

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

You need the following to configure this data collector:

- IP address of each DS array
- Read-only username and password on each DS array
- Third-party software installed on the Cloud Insights AU: IBM *dscli*
- Access validation: Run *dscli* commands using the username and password
- Port requirements: 80, 443, & 1750

Configuration

Field	Description
DS Storage	IP address or fully-qualified domain name of the DS device
User Name	User name for the DS CLI
Password	Password for the DS CLI
<i>dscli</i> executable path	Full path to the <i>dscli</i> executable

Advanced configuration

Field	Description
Inventory Poll Interval (min)	Interval between inventory polls (min). The default is 40.
Storage Display Name	Name of the IBM DS storage array
Inventory Exclude Devices	Comma-separated list of device serial numbers to exclude from inventory collection
Performance Poll Interval (sec)	The default is 300.
Performance Filter Type	Include: Data collected only from devices on list. Exclude: No data from these devices is collected
Performance Filter Device List	Comma-separated list of device IDs to include or exclude from performance collection

Troubleshooting

Some things to try if you encounter problems with this data collector:

Inventory

Problem:	Try this:
Error containing: CMUC00192E, CMUC00191E or CMUC00190E	<ul style="list-style-type: none"> * Verify credentials and IP address entered. * Try to communicate with the array through web management console https://\${ip}:8452/DS8000/Console. Replace the \${ip} with data collector configured IP.

Problem:	Try this:
Error: * Cannot run program * Error executing command	* From Cloud Insights Acquisition Unit Open a CMD * Open CLI.CFG file in CLI's home dir/lib and check property JAVA_INSTALL, edit the value to match your environment * Display Java version installed on this machine, typing: "java -version" * Ping the IP address of the IBM Storage device specified in CLI command issued. * If all the above worked fine then manually run a CLI command

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Configuring the IBM PowerVM data collector

The IBM PowerVM (SSH) data collector is used to collect information about virtual partitions running on IBM POWER hardware instances managed by a hardware management console (HMC).

Terminology

Cloud Insights acquires inventory information from the virtual partitions running on IBM POWER hardware instances. For each asset type acquired, the most common terminology used for the asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
hdisk	Virtual Disk
Managed System	Host
LPAR, VIO Server	Virtual Machine
Volume Group	Data Store
Physical Volume	LUN

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

The following requirements must be met to configure and use this data collector:

- IP address of the Hardware Management Console (HMC)
- User name and password that provide access to Hardware Management Console (HMC) through SSH
- Port requirement SSH-22
- View permission on all management systems and logical partition security domains

The user must also have View permission on HMC configurations and the ability to collect VPD information for the HMC console security grouping. The user must also be allowed Virtual IO Server Command access under the Logical Partition security grouping. It is a best practice to start from a role of an operator and

then remove all roles. Read-only users on the HMC do not have privileges to run proxied commands on AIX hosts.

- IBM best practice is to have the devices monitored by two or more HMCs. Be aware that this may cause OnCommand Insight to report duplicated devices, therefore it is highly recommended to add redundant devices to the "Exclude Devices" list in the Advanced Configuration for this data collector.

Configuration

Field	Description
Hardware Management Console (HMC) IP Address	IP address or fully-qualified domain name of the PowerVM Hardware Management Console
HMC User	User name for the Hardware Management Console
Password	Password used for the Hardware Management Console

Advanced configuration

Field	Description
Inventory Poll Interval (min)	Interval between inventory polls. The default is 20 minutes.
SSH Port	Port used for SSH to the PowerVM
Password	Password used for the Hardware Management Console
Number of Retries	Number of inventory retry attempts
Exclude Devices	Comma-separated list of device IDs or display names to exclude

Troubleshooting

Additional information on this Data Collector may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Configuring the IBM SAN Volume Controller data collector

The IBM SAN Volume Controller (SVC) data collector collects inventory and performance data using SSH, supporting a variety of devices that run the SVC operating system.

The list of supported devices includes models such as the SVC, the v7000, the v5000, and the v3700. Refer to the Cloud Insights support matrix for supported models and firmware versions.

Terminology

Cloud Insights acquires the following inventory information from the IBM SVC data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Drive	Disk
Cluster	Storage
Node	Storage Node
Mdisk Group	Storage Pool
Vdisk	Volume
Mdisk	Backend LUNs and paths

Note: These are common terminology mappings only and might not represent every case for this data collector.

Inventory Requirements

- IP address of each SVC cluster
- Port 22 available
- Read-only user name and password

Performance Requirements

- SVC Console, which is mandatory for any SVC cluster and required for the SVC discovery foundation package.
- Credentials will require administrative access level only for copying performance files from cluster nodes to the config node.
- Enable data collection by connecting to the SVC cluster by SSH and running: `svctask startstats -interval 1`

Note: Alternatively, enable data collection using the SVC management user interface.

Configuration

Field	Description
Cluster IP Addresses	IP addresses or fully-qualified domain names of the SVC storage
Inventory User Name	User name for the SVC CLI
Inventory Password	Password for the SVC CLI

Advanced configuration

Field	Description
Inventory Poll Interval (min)	Interval between inventory polls. The default is 40 minutes.
Performance Poll Interval (sec)	Interval between performance polls. The default is 300 seconds.
To clean up dumped stats files	Select this checkbox to clean up dumped stats files

Troubleshooting

Some things to try if you encounter problems with this data collector:

Problem:	Try this:
Error: "The command cannot be initiated because it was not run on the configuration node."	The command must be executed on the configuration node.

Some things to try if you encounter problems with this data collector:

Problem:	Try this:
Error: "The command cannot be initiated because it was not run on the configuration node."	The command must be executed on the configuration node.

Additional information on this Data Collector may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Configuring the IBM XIV/A9000 data collector

IBM XIV and A9000 (CLI) data collector uses the XIV command-line interface to collect inventory data while performance collection is accomplished by making SMI-S calls to the XIV/A9000 array, which runs a SMI-S provider on port 7778.

Terminology

Vendor/Model Term	Cloud Insights Term
Disk	Disk
Storage System	Storage
Storage Pool	Storage Pool
Volume	Volume

Requirements

The following requirements must be met to configure and use this data collector:

- Port requirement: TCP port 7778
- Read-only user name and password
- The XIV CLI must be installed on the AU

Performance requirements

The following are requirements for performance collection:

- SMI-S Agent 1.4 or higher
- SMI-S compatible CIMService running on array. Most XIV arrays have a CIMServer installed by default.
- User login must be provided for the CIMServer. The login must have full read access to the array configuration and properties.

- SMI-S namespace. Default is root/ibm. This is configurable in the CIMServer.
- Port Requirements: 5988 for HTTP, 5989 for HTTPS.
- Refer to the following link on how to create an account for SMI-S performance collection:
http://publib.boulder.ibm.com/infocenter/tivihelp/v4r1/index.jsp?topic=%2Fcom.ibm.tpc_V41.doc%2Ffqz0_t_adding_cim_agent.html

Configuration

Field	Description
XIV IP address	IP address or fully-qualified domain name of the XIV storage
User Name	User name for the XIV storage
Password	Password for the XIV storage
Full Path to XIV CLI Directory	Full path to the folder containing the XIV CLI
SMI-S Host IP Address	IP address of the SMI-S host

Advanced configuration

Field	Description
Inventory Poll Interval (min)	Interval between inventory polls. The default is 40 minutes.
SMI-S Protocol	Protocol used to connect to the SMI-S provider. Also displays the default port.
Override SMI-S Port	If blank, use the default port in the Connection Type field, otherwise enter the connection port to use
Username	User name for the SMI-S Provider Host
Password	Password for the SMI-S Provider Host
Performance Poll Interval (sec)	Interval between performance polls. The default is 300 seconds.

Troubleshooting

Additional information on this Data Collector may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Lenovo data collector

Cloud Insights uses the Lenovo data collector to discover inventory and performance data for Lenovo HX storage systems.

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

- Prism External IP Address
- Administrator user name and password
- TCP Port requirement: 9440

Configuration

Field	Description
Prism External IP Address	The external data services IP address for the cluster
User name	User name for the Admin account
Password	Password for the Admin account

Advanced configuration

Field	Description
TCP port	TCP Port used to connect to array. The default is 9440.
Inventory poll interval (min)	Interval between inventory polls. The default is 60 minutes.
Performance poll interval (sec)	Interval between performance polls. The default is 300 seconds.

Troubleshooting

Additional information on this Data Collector may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Microsoft

Configuring the Azure NetApp Files data collector

Cloud Insights uses the Azure NetApp Files data collector to acquire inventory and performance data.

Requirements

You need the following information to configure this data collector.

- Port requirement: 443 HTTPS
- Azure Management Rest IP (management.azure.com)
- Azure service principal client ID (user account)
- Azure service principal authentication key (user password)
- You need to set up an Azure account for Cloud Insights discovery.

Once the account is properly configured and you register the application in Azure, you will have the credentials required to discover the Azure instance with Cloud Insights. The following link describes how to set up the account for discovery:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal>

Configuration

Enter data into the data collector fields according to the table below:

Field	Description
Azure Service Principal Client ID	Sign-in ID to Azure
Azure Tenant ID	Azure Tenant ID
Azure Service Principal Authentication Key	Login authentication key
I understand Microsoft bills me for API requests	Check this to verify your understanding that Microsoft bills you for API requests made by Insight polling.

Advanced Configuration

Field	Description
Inventory Poll Interval (min)	The default is 60

Troubleshooting

- The credentials used by your ANF data collector must not have access to any Azure subscriptions that contain ANF volumes.
- If Reader access causes performance collection to fail, try granting contributor access on a resource group level.

Additional information on this Data Collector may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Microsoft Hyper-V data collector

The Microsoft Hyper-V data collector acquires inventory and performance data from the virtualized server computing environment.

Terminology

Cloud Insights acquires the following inventory information from the Microsoft Hyper-V (WMI). For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Virtual Hard Disk	Virtual Disk
Host	Host
Virtual Machine	Virtual Machine

Vendor/Model Term	Cloud Insights Term
Cluster Shared Volumes (CSV), Partition Volume	Data Store
Internet SCSI Device, Multi Path SCSI LUN	LUN
Fiber Channel Port	Port

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

The following are required to configure this data collector:

- The Hyper-V requires port 5985 opened for data collection and remote access/management.
- IP address of Clustering group node
- Local Administrator user & password on the hypervisor
- Administrative-level user account
- Windows Management Instrumentation (WMI) command, which is the default that is installed by Windows.
- Port requirements: Port 135 via WMI & Dynamic TCP ports assigned 1024-65535 for Windows 2003 and older and 49152-65535 for Windows 2008.
- DNS resolution must succeed, even if the data collector is pointed at only an IP address
- Each Hyper-V hypervisor must have “Resource Metering” turned on for every VM, on every host. This allows each hypervisor to have more data available for Cloud Insights on each guest. If this is not set, fewer performance metrics are acquired for each guest. More information on Resource metering can be found in the microsoft documentation:

[Hyper-V Resource Metering Overview](#)

[Enable-VMResourceMetering](#)



The Hyper-V data collector requires a Windows Acquisition Unit.

Configuration

Field	Description
Physical Host IP Address	The IP address or fully-qualified domain name for the physical host (hypervisor)
User Name	Administrator user name for the hypervisor
Password	Password for the hypervisor
NT Domain	The DNS name used by the nodes in the cluster

Advanced configuration

Field	Description
Inventory Poll Interval (min)	The default is 20 minutes.

Troubleshooting

Additional information on this Data Collector may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

NetApp

NetApp Cloud Connection for ONTAP 9.9+ data collector

This data collector creates a cloud connection to support data collection from ONTAP 9.9+ CVO, AFF, and FAS systems.



This data collector is [deprecated](#) as of January 1, 2023. For information on transitioning to AU-based data collection, see the [Knowledgebase](#).

Configuration

Cloud Insights collects data from ONTAP 9.9+ using a **cloud connection**, eliminating the need to install an external acquisition unit, simplifying troubleshooting, maintenance, and initial deployment. Configuration of the cloud connection for the ONTAP 9.9+ data collector requires you to copy a **Pairing Code** to the ONTAP System Manager, which will then establish a connection to your Cloud Insights environment. After the connection is established, the data collected is the same as it would be if it was collected through an acquisition unit.

This data collector supports ONTAP 9.9+ CVO, AFF, and FAS systems.

The screenshot shows the configuration steps for a cloud connection:

- 1 Generate Token
- 2 Copy Pairing Code
- 3 In a new tab, login to ONTAP System Manager (SM) for the cluster you would like to monitor and navigate to Cluster > Settings > Cloud Connections.
- 4 Click on Add Cloud Connection and paste the Pairing Code from step 2.
- 5 The connection will be established automatically with no additional user interaction. Check System Manager for error messages if connection is not established after a few minutes.

Follow these steps to configure the connection:

- Generate a unique token which will be used to establish the connection to the ONTAP system.
- Copy the Pairing Code, which includes the token. You can view the pairing code by clicking on [\[+\] Reveal Code Snippet](#).

Once you copy the pairing code, the data collector configuration screen will reveal a step 6, prompting you to wait for the connection to be established. Nothing more needs to be done on this screen until the connection is established.

6

[Return to Data Collectors](#)

 Waiting for connection from ONTAP

- In a new browser tab, log into the ONTAP System Manager and navigate to *Cluster > Settings > Cloud Connections*.
- Click *Add Cloud Connection* and paste the pairing code.
- Return to the Cloud Insights browser tab and wait for the connection to be established. Once it is established, a *Complete* button is revealed.
- Click *Complete*.

Troubleshooting

Some things to try if you encounter problems with this data collector:

Problem:	Try this:
I'm seeing the following error while trying to connect to Azure CVO: "The certificate signing request to broker/manager CA service was not completed."	Verify that your Cloud manager proxy settings are set to the Cloud Manager private IP. Cloud Manager installation may set a different proxy. Once the proxy is set to the correct IP and you reference the proxy in the Cloud Connector dialog, the connection to Cloud Insights should connect successfully.

Additional information on this Data Collector may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

NetApp Cloud Volumes ONTAP data collector

This data collector supports inventory collection from Cloud Volumes ONTAP configurations.

Configuration

Field	Description
NetApp Management IP Address	IP address for Cloud Volumens ONTAP
User Name	User name for Cloud Volumes ONTAP
Password	Password for the above user

Advanced configuration

Field	Description
Connection Type	HTTPS recommended. Also shows default port.
Override Communication Port	Port to use if not default.

Field	Description
Inventory Poll Interval (min)	Default is 60 minutes.
Inventory Concurrent Thread Count	Number of concurrent threads.
Force TLS for HTTPS	Force TLS over HTTPS
Automatically Lookup Netgroups	Automatically Lookup Netgroups
Netgroup Expansion	Select Shell or File
HTTP read timeout seconds	Default is 30 seconds
Force responses as UTF-8	Force responses as UTF-8
Performance Poll Interval (min)	Default is 900 seconds.
Performance Concurrent Thread Count	Number of concurrent threads.
Advanced Counter Data Collection	Check this to have Cloud Insights collect the advanced metrics from the list below.

Troubleshooting

Additional information on this Data Collector may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

NetApp Cloud Volumes Services for AWS data collector

This data collector supports inventory collection from NetApp Cloud Volumes Services for AWS configurations.

Configuration

Field	Description
Cloud Volumes Region	Region of the NetApp Cloud Volumes Services for AWS
API Key	Cloud Volumes API key
Secret Key	Cloud Volumes secret key

Advanced configuration

Field	Description
Inventory Poll Interval (min)	Default is 60 minutes

Troubleshooting

Some things to try if you encounter problems with this data collector:

Problem:	Try this:
<p>I received an error similar to this one: 'Failed to execute request: Connect to <AWS region endpoint>:8080 [<AWS region endpoint>/AWS region endpoint IP] failed: connect timed out: GET <a href="https://<AWS Region Endpoint">https://<AWS Region Endpoint FQDN>:8080/v1/Storage/IPRanges HTTP/1.1'</p>	<p>The proxy used by Cloud Insights to communicate with the Acquisition Unit does not communicate between Cloud Insights and the Data Collector itself. Here are a few things you can try:</p> <p>Ensure that the acquisition unit is able to resolve the fqdn and reach the required port. Confirm that a proxy is not required to reach the specified endpoint in the error message. Curl can be used to test the communication between the acquisition unit and the endpoint. Make sure that you are not using a Proxy for this test.</p> <p>Example:</p> <pre>root@acquisitionunit# curl -s -H accept:application/json -H "Content-type: application/json" -H api-key:<api key used in the data collector credentials -H secret-key:<secret key used in the data collector credentials> -X GET <a href="https://<AWS Regional Endpoint">https://<AWS Regional Endpoint:8080/v1/Storage/IPRanges</pre> <p>See this NetApp KB article.</p>

Additional information on this Data Collector may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

NetApp Config Advisor data collector

This data collector acquires configuration data from storage systems running ONTAP and connected switches using read-only calls. This data collector also runs configuration validation and health checks on the whole stack of ONTAP cluster configuration to identify cabling, configuration, resiliency, availability and security issues.



This data collector is [deprecated](#).

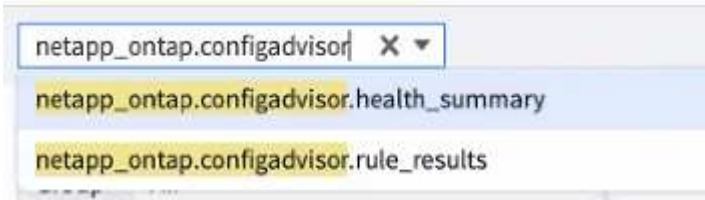
Terminology

Cloud Insights acquires configuration data from ONTAP and switches with the Config Advisor data collector. For each asset type acquired, the most common terminology used for the asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Disk	Disk
Switch	Switch
Cluster	Storage
Node	Storage Node

Vendor/Model Term	Cloud Insights Term
Aggregate	Storage Pool
LUN	Volume
Volume	Internal Volume

In addition, note that Config Advisor metrics will be available in dashboard and other queries with the `netapp_ontap.configadvisor` tag.



Config Advisor Terminology

The following terms apply to objects or references that you might find on Config Advisor dashboards.

Device Summary

- Model – A comma-delimited list of the unique, discrete node model names within this cluster. If all the nodes in the clusters are the same model type, just one model name will appear.
- Device Type/Type – type of the device in data source – Storage Controller/Switch
- Vendor/Subtype – same Vendor name you would see if you were configuring a new data source.
- Serial number – The array serial number. On cluster architecture storage systems like ONTAP Data Management, this serial number may be less useful than the individual “Storage Nodes” serial numbers.
- Hostname –hostname(s) as configured in the data source.
- Version – OS or firmware version.

Rule Results

- Rule – A check that is run against the system analysing deviation in configuration from recommended practices or identifying known issues.
- Rule Name – short name for the rule or check that is run.
- Rule ID – identifier for the rule.
- Target – component on which the rule is applied. It would be cluster name, node name or switch name.
- Impact – Impact of the risk on the system. Impact levels are categorized as below
 - High Impact: Potential loss of data access or prolonged loss of node redundancy
 - Medium Impact: Performance degradation or short-term loss of node redundancy.
 - Low Impact: Low impact scenarios
 - Best Practice: Deviations from documented Best Practices
- Description – Brief description of the error.
- Details – detailed description of the error listing the components impacted
 - Recommendations – Links to KB articles or NetApp documentation providing additional details on the

risk or remediation.

Requirements

The following are requirements to configure and use this data collector:

- You must have access to an administrator account configured for read-only access for SSH and ONTAPI calls on ONTAP.
- You must have access to an administrator account configured for read-only access for SSH calls on switches if they are part of collection
- Account details include username and password. Optionally can pass the SSH private key if ONTAP is configured for SSH key based authentication or Multi Factor Authentication (MFA)
- Port requirements: 22, 80 or 443
- Account permissions:
 - Read only role name to ssh or/and ontapi application to the default Vserver
 - Admin account with at least read-only permission on switches

Configuration

Field	Description
NetApp Management IP	IP address or fully-qualified domain name of the NetApp cluster
User Name	User name for NetApp cluster
Password	Password for NetApp cluster

Advanced configuration

Field	Description
Enable MFA for ONTAP	Check this to enable Multi-Factor Authentication on ONTAP
SSH Private Key	Paste the SSH private key content if ONTAP is using SSH key authentication or MFA
Connection type	Choose HTTP (default port 80) or HTTPS (default port 443). The default is HTTPS
ONTAP SSH Port	Allows to specify custom SSH port for ONTAP connection
Switch SSH Port	Allows to specify custom SSH port for Switch connection
Poll Interval (min)	Default is 1440 minutes or 24 hours. Can set minimum up to 60 min

Supported Operating Systems

Config Advisor can run on following operating systems. If collector is installed on an Acquisition Unit with Operating System not in this list, collections would fail.

- Windows 10 (64-bit)
- Windows 2012 R2 Server (64-bit)
- Windows 2016 Server (64-bit)
- Windows 2019 Server (64-bit)
- Red Hat Enterprise Linux (RHEL) 7.7 and later (64-bit)
- Ubuntu 14.0 and later

Support and Video

Watch these videos to learn how to install the data collector and use dashboards to get the most out of Config Advisor in Cloud Insights:

Installing and configuring the data collector:

[!\[\]\(0df4cecf179a5ba653877b41d241767b_img.jpg\) | Installing and Configuring the Config Advisor data collector](#)

Creating a Config Advisor dashboard:

[!\[\]\(8fd41f21be8d48dd6683445409d74a3e_img.jpg\) | Using dashboards to view Config Advisor data](#)

Other support

For other questions associated with Config Advisor, open a ticket from the Config Advisor Tool by clicking on Help → Open Support Ticket.

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

NetApp ONTAP Data Management Software data collector

This data collector acquires inventory and performance data from storage systems running ONTAP using read-only API calls from an ONTAP account. This data collector also creates a record in the cluster application registry to accelerate support.

Terminology

Cloud Insights acquires inventory and performance data from the ONTAP data collector. For each asset type acquired, the most common terminology used for the asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Disk	Disk
Raid Group	Disk Group
Cluster	Storage
Node	Storage Node
Aggregate	Storage Pool
LUN	Volume
Volume	Internal Volume

ONTAP Data Management Terminology

The following terms apply to objects or references that you might find on ONTAP Data Management storage asset landing pages. Many of these terms apply to other data collectors as well.

Storage

- Model – A comma-delimited list of the unique, discrete node model names within this cluster. If all the nodes in the clusters are the same model type, just one model name will appear.
- Vendor – same Vendor name you would see if you were configuring a new data source.
- Serial number – The array serial number. On cluster architecture storage systems like ONTAP Data Management, this serial number may be less useful than the individual “Storage Nodes” serial numbers.
- IP – generally will be the IP(s) or hostname(s) as configured in the data source.
- Microcode version – firmware.
- Raw Capacity – base 2 summation of all the physical disks in the system, regardless of their role.
- Latency – a representation of what the host facing workloads are experiencing, across both reads and writes. Ideally, Cloud Insights is sourcing this value directly, but this is often not the case. In lieu of the array offering this up, Cloud Insights is generally performing an IOPs-weighted calculation derived from the individual internal volumes’ statistics.
- Throughput – aggregated from internal volumes.
Management – this may contain a hyperlink for the management interface of the device. Created programmatically by the Cloud Insights data source as part of inventory reporting.

Storage Pool

- Storage – what storage array this pool lives on. Mandatory.
- Type – a descriptive value from a list of an enumerated list of possibilities. Most commonly will be “Aggregate” or “RAID Group”.
- Node – if this storage array’s architecture is such that pools belong to a specific storage node, its name will be seen here as a hyperlink to its own landing page.
- Uses Flash Pool – Yes/No value – does this SATA/SAS based pool have SSDs used for caching acceleration?
- Redundancy – RAID level or protection scheme. RAID_DP is dual parity, RAID_TP is triple parity.
- Capacity – the values here are the logical used, usable capacity and the logical total capacity, and the percentage used across these.
- Over-committed capacity – If by using efficiency technologies you have allocated a sum total of volume or internal volume capacities larger than the logical capacity of the storage pool, the percentage value here will be greater than 0%.
- Snapshot – snapshot capacities used and total, if your storage pool architecture dedicates part of its capacity to segments areas exclusively for snapshots. ONTAP in MetroCluster configurations are likely to exhibit this, while other ONTAP configurations are less so.
- Utilization – a percentage value showing the highest disk busy percentage of any disk contributing capacity to this storage pool. Disk utilization does not necessarily have a strong correlation with array performance – utilization may be high due to disk rebuilds, deduplication activities, etc in the absence of host driven workloads. Also, many arrays’ replication implementations may drive disk utilization while not showing as internal volume or volume workload.
- IOPS – the sum IOPs of all the disks contributing capacity to this storage pool.

Throughput – the sum throughput of all the disks contributing capacity to this storage pool.

Storage Node

- Storage – what storage array this node is part of. Mandatory.
- HA Partner – on platforms where a node will fail over to one and only one other node, it will generally be seen here.
- State – health of the node. Only available when the array is healthy enough to be inventoried by a data source.
- Model – model name of the node.
- Version – version name of the device.
- Serial number – The node serial number.
- Memory – base 2 memory if available.
- Utilization – On ONTAP, this is a controller stress index from a proprietary algorithm. With every performance poll, a number between 0 and 100% will be reported that is the higher of either WAFL disk contention, or average CPU utilization. If you observe sustained values > 50%, that is indicative of undersizing – potentially a controller/node not large enough or not enough spinning disks to absorb the write workload.
- IOPS – Derived directly from ONTAP ZAPI calls on the node object.
- Latency – Derived directly from ONTAP ZAPI calls on the node object.
- Throughput – Derived directly from ONTAP ZAPI calls on the node object.
- Processors – CPU count.

Requirements

The following are requirements to configure and use this data collector:

- You must have access to an Administrator account configured for read-only API calls.
- Account details include username and password.
- Port requirements: 80 or 443
- Account permissions:
 - Read only role name to ontapi application to the default Vserver
 - You may require additional optional write permissions. See the Note About Permissions below.
- ONTAP License requirements:
 - FCP license and mapped/masked volumes required for fibre-channel discovery

Configuration

Field	Description
NetApp Management IP	IP address or fully-qualified domain name of the NetApp cluster
User Name	User name for NetApp cluster
Password	Password for NetApp cluster

Advanced configuration

Field	Description
Connection type	Choose HTTP (default port 80) or HTTPS (default port 443). The default is HTTPS
Override Communication Port	Specify a different port if you do not want to use the default
Inventory Poll Interval (min)	Default is 60 minutes.
For TLS for HTTPS	Only allow TLS as protocol when using HTTPS
Automatically Lookup Netgroups	Enable the automatic netgroup lookups for export policy rules
Netgroup Expansion	Netgroup Expansion Strategy. Choose <i>file</i> or <i>shell</i> . The default is <i>shell</i> .
HTTP read timeout seconds	Default is 30
Force responses as UTF-8	Forces data collector code to interpret responses from the CLI as being in UTF-8
Performance Poll Interval (sec)	Default is 900 seconds.
Advanced Counter Data Collection	Enable ONTAP integration. Select this to include ONTAP Advanced Counter data in polls. Choose the desired counters from the list.

A Note About Permissions

Since a number of Cloud Insights' ONTAP dashboards rely on advanced ONTAP counters, you must enable **Advanced Counter Data Collection** in the data collector Advanced Configuration section.

You should also ensure that write permission to the ONTAP API is enabled. This typically requires an account at the cluster level with the necessary permissions.

To create a local account for Cloud Insights at the cluster level, log in to ONTAP with the Cluster management Administrator username/password, and execute the following commands on the ONTAP server:

1. Before you begin, you must be signed in to ONTAP with an *Administrator* account, and *diagnostic-level commands* must be enabled.
2. Create a read-only role using the following commands.

```
security login role create -role ci_READONLY -cmddirname DEFAULT -access readonly
security login role create -role ci_READONLY -cmddirname security -access readonly
security login role create -role ci_READONLY -access all -cmddirname {cluster application-record create}
```

3. Create the read-only user using the following command. Once you have executed the create command, you will be prompted to enter a password for this user.

```
security login create -username ci_user -application ontapi  
-authentication-method password -role ci_READONLY
```

If AD/LDAP account is used, the command should be

```
security login create -user-or-group-name DOMAIN\aduser/adgroup  
-application ontapi -authentication-method domain -role ci_READONLY
```

The resulting role and user login will look something like the following. Your actual output may vary:

```
Role Command/ Access  
Vserver Name Directory Query Level  
-----  
cluster1 ci_READONLY DEFAULT read only  
cluster1 ci_READONLY security readonly
```

```
cluster1::security login> show  
Vserver: cluster1  
Authentication Acct  
UserName Application Method Role Name Locked  
----- ----- ----- -----  
ci_user ontapi password ci_READONLY no
```

Troubleshooting

Some things to try if you encounter problems with this data collector:

Inventory

Problem:	Try this:
Receive 401 HTTP response or 13003 ZAPI error code and ZAPI returns "Insufficient privileges" or "not authorized for this command"	Check username and password, and user privileges/permissions.
Cluster version is < 8.1	Cluster minimum supported version is 8.1. Upgrade to minimum supported version.
ZAPI returns "cluster role is not cluster_mgmt LIF"	AU needs to talk to cluster management IP. Check the IP and change to a different IP if necessary
Error: "7 Mode filers are not supported"	This can happen if you use this data collector to discover 7 mode filer. Change IP to point to cdot cluster instead.

Problem:	Try this:
ZAPI command fails after retry	AU has communication problem with the cluster. Check network, port number, and IP address. User should also try to run a command from command line from the AU machine.
AU failed to connect to ZAPI via HTTP	Check whether ZAPI port accepts plaintext. If AU tries to send plaintext to an SSL socket, the communication fails.
Communication fails with SSLEException	AU is attempting to send SSL to a plaintext port on a filer. Check whether the ZAPI port accepts SSL, or use a different port.
Additional Connection errors: ZAPI response has error code 13001, "database is not open" ZAPI error code is 60 and response contains "API did not finish on time" ZAPI response contains "initialize_session() returned NULL environment" ZAPI error code is 14007 and response contains "Node is not healthy"	Check network, port number, and IP address. User should also try to run a command from command line from the AU machine.

Performance

Problem:	Try this:
"Failed to collect performance from ZAPI" error	This is usually due to perf stat not running. Try the following command on each node: <i>> system node systemshell -node * -command "spmctl -h cmd -stop; spmctl -h cmd -exec"</i>

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

NetApp Data ONTAP operating in 7-Mode data collector

For storage systems using Data ONTAP software operating in 7-Mode, you use the 7-mode data collector, which uses the CLI to obtain capacity and performance data.

Terminology

Cloud Insights acquires the following inventory information from the NetApp 7-mode data collector. For each asset type acquired, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:



This data collector is [deprecated](#).

Vendor/Model Term	Cloud Insights Term
Disk	Disk
Raid Group	Disk Group
Filer	Storage
Filer	Storage Node
Aggregate	Storage Pool
LUN	Volume
Volume	Internal Volume

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

You need the following to configure and use this data collector:

- IP addresses of the FAS storage controller and partner.
- Port 443
- A custom admin level username and password for controller and partner controller with the following role capabilities for 7-Mode:
 - "api-*": Use this to allow OnCommand Insight to execute all NetApp storage API commands.
 - "login-http-admin": Use this to allow OnCommand Insight to connect to the NetApp storage via HTTP.
 - "security-api-vfiler": Use this to allow OnCommand Insight to execute NetApp storage API commands to retrieve vFiler unit information.
 - "cli-options": Use this to read storage system options.
 - "cli-lun": Access these commands for managing LUNs. Displays the status (LUN path, size, online/offline state, and shared state) of the given LUN or class of LUNs.
 - "cli-df": Use this to display free disk space.
 - "cli-ifconfig": Use this to display interfaces and IP addresses.

Configuration

Field	Description
Address of storage system	IP address or fully-qualified domain name for the NetApp storage system
User Name	User name for the NetApp storage system
Password	Password for the NetApp storage system
Address of HA Partner in Cluster	IP address or fully-qualified domain name for the HA Partner
User Name of HA Partner in Cluster	User name for the HA partner
Password of HA Partner Filer in Cluster	Password for the HA Partner

Advanced configuration

Field	Description
Inventory Poll Interval (min)	Interval between inventory polls. The default is 20 minutes.
Connection Type	HTTPS or HTTP, also displays the default port
Override Connection Port	If blank, use the default port in the Connection Type field, otherwise enter the connection port to use
Performance Poll Interval (sec)	Interval between performance polls. The default is 300 seconds.

Storage systems connection

As an alternative to using the default administrative user for this data collector, you can configure a user with administrative rights directly on the NetApp storage systems so that this data collector can acquire data from NetApp storage systems.

Connecting to NetApp storage systems requires that the user, who is specified when acquiring the main pfiler (on which the storage system exist), meet the following conditions:

- The user must be on vfiler0 (root filer/pfiler).

Storage systems are acquired when acquiring the main pfiler.

- The following commands define the user role capabilities:

- "api-*": Use this to allow Cloud Insights to execute all NetApp storage API commands.

This command is required to use the ZAPI.

- "login-http-admin": Use this to allow Cloud Insights to connect to the NetApp storage via HTTP. This command is required to use the ZAPI.
 - "security-api-vfiler": Use this to allow Cloud Insights to execute NetApp storage API commands to retrieve vFiler unit information.
 - "cli-options": For "options" command and used for partner IP and enabled licenses.
 - "cli-lun": Access these command for managing LUNs. Displays the status (LUN path, size, online/offline state, and shared state) of the given LUN or class of LUNs.
 - "cli-df": For "df -s", "df -r", "df -A -r" commands and used to display free space.
 - "cli-ifconfig": For "ifconfig -a" command and used for getting filer IP address.
 - "cli-rdfile": For "rdfile /etc/netgroup" command and used for getting netgroups.
 - "cli-date": For "date" command and used to get full date for getting Snapshot copies.
 - "cli-snap": For "snap list" command and used for getting Snapshot copies.

If cli-date or cli-snap permissions are not provided, acquisition can finish, but Snapshot copies are not reported.

To acquire a 7-Mode data source successfully and generate no warnings on the storage system, you should use one of the following command strings to define your user roles. The second string listed here is a streamlined version of the first:

- login-http-admin,api-* ,security-api-vfile,cli-rdfile,cli-options,cli-df,cli-lun,cli-ifconfig,cli-date,cli-snap,...
- login-http-admin,api-* ,security-api-vfile,cli-

Troubleshooting

Some things to try if you encounter problems with this data collector:

Inventory

Problem:	Try this:
Receive 401 HTTP response or 13003 ZAPI error code and ZAPI returns “Insufficient privileges” or “not authorized for this command”	Check username and password, and user privileges/permissions.
“Failed to execute command” error	<p>Check whether the user has the following permission on the device:</p> <ul style="list-style-type: none"> • api-* • cli-date • cli-df • cli-ifconfig • cli-lun • cli-operations • cli-rdfile • cli-snap • login-http-admin • security-api-vfiler <p>Also check if the ONTAP version is supported by Cloud Insights and verify if the credentials used match device credentials</p>
Cluster version is < 8.1	Cluster minimum supported version is 8.1. Upgrade to minimum supported version.
ZAPI returns "cluster role is not cluster_mgmt LIF"	AU needs to talk to cluster management IP. Check the IP and change to a different IP if necessary
Error: “7 Mode filers are not supported”	This can happen if you use this data collector to discover 7 mode filer. Change IP to point to cdot filer instead.
ZAPI command fails after retry	AU has communication problem with the cluster. Check network, port number, and IP address. User should also try to run a command from command line from the AU machine.
AU failed to connect to ZAPI	Check IP/port connectivity and assert ZAPI configuration.
AU failed to connect to ZAPI via HTTP	Check whether ZAPI port accepts plaintext. If AU tries to send plaintext to an SSL socket, the communication fails.
Communication fails with SSLEException	AU is attempting to send SSL to a plaintext port on a filer. Check whether the ZAPI port accepts SSL, or use a different port.

Problem:	Try this:
Additional Connection errors: ZAPI response has error code 13001, "database is not open"	Check network, port number, and IP address. User should also try to run a command from command line from the AU machine.
ZAPI error code is 60 and response contains "API did not finish on time"	
ZAPI response contains "initialize_session() returned NULL environment"	
ZAPI error code is 14007 and response contains "Node is not healthy"	
Socket timeout error with ZAPI	Check filer connectivity and/or increase timeout.
"C Mode clusters are not supported by the 7 Mode data source" error	Check IP and change the IP to a 7 Mode cluster.
"Failed to connect to vFiler" error	Check that the acquiring user capabilities include the following at a minimum: api-* security-api-vfiler login-http-admin Confirm that filer is running minimum ONTAPI version 1.7.

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

NetApp E-Series data collector

The NetApp E-Series data collector gathers inventory and performance data. The collector supports firmware 7.x+ using the same configurations and reporting the same data.

Terminology

Cloud insight acquires the following inventory information from the NetApp E-Series data collector. For each asset type acquired, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Disk	Disk
Volume Group	Disk Group
Storage Array	Storage
Controller	Storage Node
Volume Group	Storage Pool
Volume	Volume

Note: These are common terminology mappings only and might not represent every case for this data collector.

E-Series Terminology (Landing Page)

The following terms apply to objects or references that you might find on NetApp E-Series asset landing pages. Many of these terms apply to other data collectors as well.

Storage

- Model – model name of the device.
- Vendor – same Vendor name you would see if you were configuring a new datasource
- Serial number – The array serial number. On cluster architecture storage systems like NetApp Clustered Data Ontap, this serial number may be less useful than the individual “Storage Nodes” serial numbers
- IP – generally will be the IP(s) or hostname(s) as configured in the data source
- Microcode version – firmware
- Raw Capacity – base 2 summation of all the physical disks in the system, regardless of their role
- Latency – a representation of what the host facing workloads are experiencing, across both reads and writes. Ideally, Cloud Insights is sourcing this value directly, but this is often not the case. In lieu of the array offering this up, Cloud Insights is generally performing an IOPs-weighted calculation derived from the individual volumes’ statistics.
- Throughput – the array’s total host facing throughput. Ideally sourced directly from the array, if unavailable, Cloud Insights is summing the volumes’ throughput to derive this value
- Management – this may contain a hyperlink for the management interface of the device. Created programmatically by the Cloud Insights datasource as part of inventory reporting

Storage Pool

- Storage – what storage array this pool lives on. Mandatory
- Type – a descriptive value from a list of an enumerated list of possibilities. Most commonly will be “Thin Provisioning” or “RAID Group”
- Node – if this storage array’s architecture is such that pools belong to a specific storage node, its name will be seen here as a hyperlink to its own landing page
- Uses Flash Pool – Yes/No value
- Redundancy – RAID level or protection scheme. E-Series reports “RAID 7” for DDP pools
- Capacity – the values here are the logical used, usable capacity and the logical total capacity, and the percentage used across these. These values both include E-Series “preservation” capacity, resulting both in numbers and the percentage being higher than what the E-Series own user interface may show
- Over-committed capacity – If via efficiency technologies you have allocated a sum total of volume or internal volume capacities larger than the logical capacity of the storage pool, the percentage value here will be greater than 0%.
- Snapshot – snapshot capacities used and total, if your storage pool architecture dedicates part of its capacity to segments areas exclusively for snapshots
- Utilization – a percentage value showing the highest disk busy percentage of any disk contributing capacity to this storage pool. Disk utilization does not necessarily have a strong correlation with array performance – utilization may be high due to disk rebuilds, deduplication activities, etc in the absence of host driven

workloads. Also, many arrays' replication implementations may drive disk utilization while not showing as volume workload.

- IOPS – the sum IOPs of all the disks contributing capacity to this storage pool. If disk IOPs is not available on a given platform, this value will be sourced from the sum of volume IOPs for all the volumes sitting on this storage pool
- Throughput – the sum throughput of all the disks contributing capacity to this storage pool. If disk throughput is not available on a given platform, this value will be sourced from the sum of volume throughout for all the volumes sitting on this storage pool

Storage Node

- Storage – what storage array this node is part of. Mandatory
- HA Partner – on platforms where a node will fail over to one and only one other node, it will generally be seen here
- State – health of the node. Only available when the array is healthy enough to be inventoried by a data source
- Model – model name of the node
- Version – version name of the device.
- Serial number – The node serial number
- Memory – base 2 memory if available
- Utilization – Generally a CPU utilization number, or in the case of NetApp Ontap, a controller stress index. Utilization is not currently available for NetApp E-Series
- IOPS – a number representing the host driven IOPs on this controller. Ideally sourced directly from the array, if unavailable, it will be calculated by summing all the IOPs for volumes that belong exclusively to this node.
- Latency – a number representing the typical host latency or response time on this controller. Ideally sourced directly from the array, if unavailable, it will be calculated by performing an IOPs weighted calculation from volumes that belong exclusively to this node.
- Throughput – a number representing the host driven throughput on this controller. Ideally sourced directly from the array, if unavailable, it will be calculated by summing all the throughput for volumes that belong exclusively to this node.
- Processors – CPU count

Requirements

- The IP address of each controller on the array
- Port requirement 2463

Configuration

Field	Description
Comma-separated list of Array SANtricity Controller IPs	IP addresses and/or fully-qualified domain names for the array controllers

Advanced configuration

Field	Description
Inventory Poll Interval (min)	Default is 30 minutes
Performance Poll Interval up to 3600 seconds	Default is 300 seconds

Troubleshooting

Additional information on this data collector may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Configuring the NetApp HCI Management server data collector

The NetApp HCI Management server data collector collects NetApp HCI Host information and requires read-only privileges on all objects within the Management server.

This data collector acquires from the **NetApp HCI Management server only**. To collect data from the storage system, you must also configure the [NetApp SolidFire](#) data collector.

Terminology

Cloud Insights acquires the following inventory information from this data collector. For each asset type acquired, the most common terminology used for the asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Virtual disk	Disk
Host	Host
Virtual machine	Virtual machine
Data store	Data store
LUN	Volume
Fibre channel port	Port

These are common terminology mappings only and might not represent every case for this data collector.

Requirements

The following information is required to configure this data collector:

- IP address of the NetApp HCI Management server
- Read-only username and password for the NetApp HCI Management server
- Read only privileges on all objects in the NetApp HCI Management server.
- SDK access on the NetApp HCI Management server – normally already set up.
- Port requirements: http-80 https-443
- Validate access:

- Log into the NetApp HCI Management server using above username and password
- Verify SDK enabled: telnet <vc_ip> 443

Setup and connection

Field	Description
Name	Unique name for the data collector
Acquisition unit	Name of acquisition unit

Configuration

Field	Description
NetApp HCI Storage Cluster MVIP	Management Virtual IP Address
SolidFire Management Node (mNode)	Management Node IP Address
User name	User name used to access the NetApp HCI Management server
Password	Password used to access the NetApp HCI Management server
VCenter User Name	User name for VCenter
VCenter Password	Password for VCenter

Advanced configuration

In the advanced configuration screen, check the **VM Performance** box to collect performance data. Inventory collection is enabled by default.

The following fields can be configured:

Field	Description
Inventory poll interval (min)	Default is 20
Filter VMs by	Select CLUSTER, DATACENTER, or ESX HOST
Choose 'Exclude' or 'Include' to Specify a List	Specify Whether to Include or Exclude VMs
Filter Device List	List of VMs to filter (comma separated, or semicolon separated if comma is used in the value) for for Filtering by ESX_HOST, CLUSTER, and DATACENTER Only
Performance poll interval (sec)	Default is 300

Troubleshooting

Some things to try if you encounter problems with this data collector:

Inventory

Problem:	Try this:
Error: Include list to filter VMs cannot be empty	If Include List is selected, please list valid DataCenter, Cluster, or Host names to filter VMs
Error: Failed to instantiate a connection to VirtualCenter at IP	<p>Possible solutions:</p> <ul style="list-style-type: none"> * Verify credentials and IP address entered. * Try to communicate with Virtual Center using Infrastructure Client. * Try to communicate with Virtual Center using Managed Object Browser (e.g MOB).
Error: VirtualCenter at IP has non-conform certificate that JVM requires	<p>Possible solutions:</p> <ul style="list-style-type: none"> * Recommended: Re-generate certificate for Virtual Center by using stronger (e.g. 1024-bit) RSA key. * Not Recommended: Modify the JVM java.security configuration to leverage the constraint jdk.certpath.disabledAlgorithms to allow 512-bit RSA key. See JDK 7 update 40 release notes at "http://www.oracle.com/technetwork/java/javase/7u40-relnotes-2004172.html"

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

NetApp SolidFire All-Flash Array data collector

The NetApp SolidFire All-Flash Array data collector supports inventory and performance collection from both iSCSI and Fibre Channel SolidFire configurations.

The SolidFire data collector utilizes the SolidFire REST API. The acquisition unit where the data collector resides needs to be able to initiate HTTPS connections to TCP port 443 on the SolidFire cluster management IP address. The data collector needs credentials capable of making REST API queries on the SolidFire cluster.

Terminology

Cloud Insights acquires the following inventory information from the NetApp SolidFire All-Flash Array data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Drive	Disk
Cluster	Storage
Node	Storage Node
Volume	Volume
Fibre channel port	Port
Volume Access Group, LUN Assignment	Volume Map
iSCSI Session	Volume Mask

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

The following are requirements for configuring this data collector:

- Management Virtual IP Address
- Read-only username and credentials
- Port 443

Configuration

Field	Description
Management Virtual IP Address (MVIP)	Management Virtual IP address of the SolidFire Cluster
User Name	Name used to log into the SolidFire cluster
Password	Password used to log into the SolidFire cluster

Advanced configuration

Field	Description
Connection Type	Choose connection type
Communication Port	Port used for NetApp API
Inventory Poll Interval (min)	Default is 20 minutes
Performance Poll Interval (sec)	Default is 300 seconds

Troubleshooting

When SolidFire reports an error it is displayed in Cloud Insights as follows:

An error message was received from a SolidFire device while trying to retrieve data. The call was <method>(<parameterString>). The error message from the device was (check the device manual): <message>

Where:

- The <method> is an HTTP method, such as GET or PUT.
- The <parameterString> is a comma separated list of parameters that were included in the REST call.
- The <message> is whatever the device returned as the error message.

Additional information on this Data Collector may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

NetApp StorageGRID data collector

The NetApp StorageGRID data collector supports inventory and performance collection from StorageGRID configurations.



StorageGRID is metered at a different Raw TB to Managed Unit rate. Every 40 TB of unformatted StorageGRID capacity is charged as 1 [Managed Unit \(MU\)](#).

Terminology

Cloud Insights acquires the following inventory information from the NetApp StorageGRID collector. For each asset type acquired, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
StorageGRID	Storage
Node	Node
Tenant	Storage Pool
Bucket	Internal Volume

Requirements

The following are requirements for configuring this data source:

- StorageGRID Host IP Address
- A username and password for a user that has had the Metric Query and Tenant Access roles assigned
- Port 443

Configuration

Field	Description
StorageGRID Host IP Address	Management Virtual IP address of the StorageGRID appliance
User Name	Name used to log into the StorageGRID appliance
Password	Password used to log into the StorageGRID appliance

Advanced configuration

Field	Description
Inventory Poll Interval (min)	Default is 60 minutes
performance Poll Interval (sec)	Default is 900 seconds

Single Sign-On (SSO)

The [StorageGRID](#) firmware versions have corresponding API versions; 3.0 API and newer versions support single sign-on (SSO) login.

Firmware version	API version	Support single sign on (SSO)
11.1	2	No

11.2	3.0	Yes
11.5	3.3	Yes

Troubleshooting

Additional information on this Data Collector may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Nutanix NX data collector

Cloud Insights uses the Nutanix data collector to discover inventory and performance data for Nutanix NX storage systems.

Terminology

Cloud Insights acquires the following inventory information from the Nutanix data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Storage Pool	Storage Pool
Nutanix Container	Internal Volume
Nutanix Container	File Share
NFS Share	Share

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

- The external data services IP address for the cluster
- Read-only user name and password, unless volume_groups are in use, in which case, Admin user name and password are required
- Port requirement: HTTPS 443

Configuration

Field	Description
Prism External IP Address	The external data services IP address for the cluster
User name	User name for the Admin account
Password	Password for the Admin account

Advanced configuration

Field	Description
TCP port	TCP Port used to connect to Nutanix array. The default is 9440.
Inventory poll interval (min)	Interval between inventory polls. The default is 60 minutes.
Performance poll interval(sec)	Interval between performance polls. The default is 300 seconds.

Troubleshooting

Additional information on this Data Collector may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

OpenStack data collector

The OpenStack (REST API / KVM) data collector acquires inventory data for all OpenStack instances, and optionally, VM performance data.

Requirements

- IP address of the OpenStack controller
- OpenStack admin role credential and sudo access to the Linux KVM hypervisor. If you are not using the admin account or admin equivalent privileges, you will need to use trial and error to identify the default policies to relax for your data collector userid.
- The OpenStack Ceilometer module must be installed and configured for performance collection. Configuring the Ceilometer is done by editing the nova.conf file for each hypervisor and then restarting the Nova Compute service on each hypervisor. The option name changes for different releases of OpenStack:
 - Icehouse
 - Juno
 - Kilo
 - Liberty
 - Mitaka
 - Newton
 - Ocata
- For CPU stats, “compute_monitors=ComputeDriverCPUMonitor” needs to be turned on in /etc/nova/nova.conf on compute nodes.
- Port requirements:
 - 5000 for http and 13000 for https, for the Keystone service
 - 22 for KVM SSH
 - 8774 for Nova Compute Service
 - 8776 for Cinder Block Service
 - 8777 for Ceilometer Performance Service

- 9292 for Glance Image Service

Note The port binds to the specific service, and the service may run on the controller or another host in larger environments.

Configuration

Field	Description
OpenStack Controller IP Address	IP address or fully-qualified domain name of the OpenStack Controller
OpenStack Administrator	User name for an OpenStack Admin
OpenStack Password	Password used for the OpenStack Admin
OpenStack Administrator Tenant	OpenStack Administrator Tenant name
KVM Sudo User	KVM Sudo User name
Choose 'Password' or 'OpenSSH Key File' to specify credential type	Credential type used to connect to the device via SSH
Full Path to Inventory Private Key	Full Path to Inventory Private Key
KVM Sudo Password	KVM Sudo Password

Advanced configuration

Field	Description
Enable hypervisor inventory discovery through SSH	Check this to enable hypervisor inventory discovery through SSH
OpenStack Admin URL port	OpenStack Admin URL port
Use HTTPS	Check to use secure HTTP
SSH Port	Port used for SSH
SSH Process Retries	Number of inventory retry attempts
Inventory Poll Interval (min)	Interval between inventory polls. The default is 20 minutes.

Troubleshooting

Some things to try if you encounter problems with this data collector:

Inventory

Problem:	Try this:
"Configuration error" with error messages start with "Policy doesn't allow" or "You are not authorized"	* Check ip address * Check User name and password

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Oracle ZFS Storage Appliance data collector

Cloud Insights uses the Oracle ZFS Storage Appliance data collector to gather inventory and performance data.

Terminology

Cloud Insights acquires inventory information with the Oracle ZFS data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Disk (SSD)	Disk
Cluster	Storage
Controller	Storage Node
LUN	Volume
LUN Map	Volume Map
Initiator,Target	Volume Mask
Share	Internal Volume

Note: These are common terminology mappings only and might not represent every case for this data source.

Requirements

- Host names for the ZFS Controller-1 and the ZFS Controller-2
- Administrator user name and password
- Port requirement: 215 HTTP/HTTPS

Required Performance metrics

Oracle ZFS appliances give storage administrators large amounts of flexibility to capture performance statistics. Cloud Insights expects you to have *each* controller in a high availability pair configured to capture the following metrics:

- smb2.ops[share]
- nfs3.ops[share]
- nfs4.ops[share]
- nfs4-1.ops[share]

Failure to have the controller capture any or all of these will likely result in Cloud Insights not having, or underreporting, the workload on the "Internal Volumes".

Configuration

Field	Description
ZFS Controller-1 Hostname	Host name for storage controller 1
ZFS Controller-2 Hostname	Host name for storage controller 2
User name	User name for the storage system administrator user account
Password	Password for the administrator user account

Advanced configuration

Field	Description
Connection Type	HTTPS or HTTP, also displays the default port
Override Connection Port	If blank, use the default port in the Connection Type field, otherwise enter the connection port to use
Inventory poll interval	The default is 60 seconds
Performance Poll Interval (sec)	The default is 300.

Troubleshooting

Some things to try if you encounter problems with this data collector:

Inventory

Problem:	Try this:
"Invalid login credentials"	validate Zfs user account and password
"Configuration error" with error message "REST Service is disabled"	Verify REST service is enabled on this device.
"Configuration error" with error message "User unauthorized for command"	Likely due to certain roles (for example, 'advanced_analytics') are not included for the configured user <userName>. Possible Solution: * Correct the Analytics (statistic) scope for the user \${user} with the read only role: - From the Configuration → Users screen, put your mouse over the role and double click to allow editing - Select "Analytics" from the Scope drop down menu. A list of the possible properties appears. - Click the top most check box and it will select all three properties. - Click the Add button on the right side. - Click the Apply button at the top right of the pop-up window. The pop-up window will close.

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Pure Storage FlashArray data collector

Cloud Insights uses the Pure Storage FlashArray data collector to gather inventory and performance data.

Terminology

For each asset type acquired by Cloud Insights, the most common terminology used for the asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Drive (SSD)	Disk
Array	Storage
Controller	Storage Node
Volume	Volume
LUN Map	Volume Map
Initiator,Target	Volume Mask

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

- Storage system IP address
- User name and password for the Administrator account of the Pure storage system.
- Port requirement: HTTP/HTTPS 80/443

Configuration

Field	Description
FlashArray Host IP Address	IP address of the storage system
User name	User name with admin privileges
Password for the admin privileged account	Password

Advanced configuration

Field	Description
Connection type	Choose HTTP or HTTPS. Also displays the default port.
Override TCP port	If blank, use the default port in the Connection Type field, otherwise enter the connection port to use
Inventory poll interval (min)	The default is 60 minutes

Field	Description
Performance Poll Interval (sec)	The default is 300

Troubleshooting

Some things to try if you encounter problems with this data collector:

Inventory

Problem:	Try this:
"Invalid login credentials" with error messages "Policy doesn't allow" or "You are not authorized"	Validate Pure user account and password via Pure http interface

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Red Hat Virtualization data collector

Cloud Insights uses the Red Hat Virtualization data collector to gather inventory data from virtualized Linux and Microsoft Windows workloads.

Terminology

For each asset type acquired by Cloud Insights, the most common terminology used for the asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Disk	Virtual Disk
Host	Host
Virtual Machine	Virtual Machine
Storage Domain	Data Store
Logical Unit	LUN

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

- IP address of the RHEV server over port 443 via REST API
- Read-only username and password
- RHEV Version 3.0+

Configuration

Field	Description
RHEV Server IP Address	IP address of the storage system
User name	User name with admin privileges
Password for the admin privileged account	Password

Advanced configuration

Field	Description
HTTPS Communication Port	Port used for HTTPS communication to RHEV
Inventory poll interval (min)	The default is 20 minutes.

Troubleshooting

Additional information on this Data Collector may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Rubrik CDM Data Collector

Cloud Insights uses the Rubrik data collector to acquire inventory and performance data from Rubrik storage appliances.

Terminology

Cloud Insights acquires the following inventory information from the Rubrik data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Cluster	Storage, Storage Pool
Node	Storage Node
Disk	Disk

Note: These are common terminology mappings only and might not represent every case for this data source.

Requirements

The following are required to configure this data collector:

- The Cloud Insights Acquisition Unit will initiate connections to TCP port 443 to Rubrik cluster. One collector per cluster.
- Rubrik cluster IP address.
- User name and password to the cluster.
- Port requirement: HTTPS 443

Configuration

Field	Description
IP	IP address of the Rubrik cluster
User name	User name for the cluster
Password	Password for the cluster

Advanced configuration

Inventory poll interval (min)	The default is 60
Performance Poll Interval (sec)	The default is 300

Troubleshooting

Some things to try if you encounter problems with this data collector:

Inventory

Problem:	Try this:
I received a message that more than one storage is created.	Check that the cluster is configured correctly, and the collector is pointing to a single cluster.
I received a warning that disk API returned more data	Check with support to get additional data.

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Configuring the VMware vSphere data collector

The data collector for VMware vSphere collects ESX Host information and requires read-only privileges on all objects within the Virtual Center.

Terminology

Cloud Insights acquires the following inventory information from the VMware vSphere data collector. For each asset type acquired, the most common terminology used for the asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Virtual disk	Disk
Host	Host
Virtual machine	Virtual machine
Data store	Data store
LUN	Volume
Fibre channel port	Port

These are common terminology mappings only and might not represent every case for this data collector.

Requirements

The following information is required to configure this data collector:

- IP address of the Virtual Center server
- Read-only username and password in Virtual Center
- We require read only privileges on all objects within Virtual Center.
- SDK access on the Virtual Center server – normally already setup.
- Port requirements: http-80 https-443
- Validate access:
 - Log into Virtual Center Client using above username and password
 - Verify SDK enabled: telnet <vc_ip> 443

Setup and connection

Field	Description
Name	Unique name for the data collector
Acquisition unit	Name of acquisition unit

Configuration

Field	Description
Virtual center IP Address	IP address of the Virtual Center
User name	User name used to access the Virtual Center
Password	Password used to access the Virtual Center

Advanced configuration

In the advanced configuration screen, check the **VM Performance** box to collect performance data. Inventory collection is enabled by default.

The following fields can be configured:

Field	Description
Inventory poll interval (min)	Default is 20
Filter VMs	Select CLUSTER, DATACENTER, or ESX HOST
Choose 'Exclude' or 'Include' to Specify a List	Create a filter list (CLUSTER, DATACENTER, and/or ESX_HOST)
Number of retries	Default is 3
Communication port	Default is 443

Filter Device List...	<p>This list must consist of exact string matches - if you intend to filter by ESX_HOST, you must build a comma delimited list of the exact "names" of your ESX hosts as reported in both Cloud Insights and vSphere. These "names" may be either IP addresses, simple hostnames, or fully qualified domain names (FQDNs) - this is determined by how these hosts were named when they were originally added to vSphere.</p> <p>When filtering by CLUSTER, use the Cloud Insights-style cluster names as reported by CI on hypervisors - Cloud Insights prepends the vSphere cluster name with the vSphere datacenter name and a forward slash - "DC1/clusterA" is the cluster name Cloud Insights would report on a hypervisor in clusterA within data center DC1.</p>
Performance poll interval (sec)	Default is 300

Troubleshooting

Some things to try if you encounter problems with this data collector:

Inventory

Problem:	Try this:
Error: Include list to filter VMs cannot be empty	If Include List is selected, please list valid DataCenter, Cluster, or Host names to filter VMs
Error: Failed to instantiate a connection to VirtualCenter at IP	<p>Possible solutions:</p> <ul style="list-style-type: none"> * Verify credentials and IP address entered. * Try to communicate with Virtual Center using VMware Infrastructure Client. * Try to communicate with Virtual Center using Managed Object Browser (e.g MOB).
Error: VirtualCenter at IP has non-conform certificate that JVM requires	<p>Possible solutions:</p> <ul style="list-style-type: none"> * Recommended: Re-generate certificate for Virtual Center by using stronger (e.g. 1024-bit) RSA key. * Not Recommended: Modify the JVM java.security configuration to leverage the constraint jdk.certpath.disabledAlgorithms to allow 512-bit RSA key. See JDK 7 update 40 release notes at "http://www.oracle.com/technetwork/java/javase/7u40-relnotes-2004172.html"

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Data Collector Reference - Services

Node Data Collection

Cloud Insights gathers metrics from the node on which you install an agent.

Installation

1. From **Admin > Data Collectors**, choose an operating system/platform. Note that installing any integration data collector (Kubernetes, Docker, Apache, etc.) will also configure node data collection.
2. Follow the instructions to configure the agent. The instructions vary depending on the type of Operating System or Platform you are using to collect data.

Objects and Counters

The following objects and their counters are collected as Node metrics:

Object:	Identifiers:	Attributes:	Datapoints:
Node Filesystem	Node UUID Device Path Type	Node IP Node Name Node OS Mode	Free Inodes Free Inodes Total Inodes Used Total Used Total Used
Node Disk	Node UUID Disk	Node IP Node Name Node OS	IO Time Total IOPS In Progress Read Bytes (per sec) Read Time Total Reads (per sec) Weighted IO Time Total Write Bytes (per sec) Write Time Total Writes (per sec) Current Disk Queue Length Write Time Read Time IO Time
Node CPU	Node UUID CPU	Node IP Node Name Node OS	System CPU Usage User CPU Usage Idle CPU Usage Processor CPU Usage Interrupt CPU Usage DPC CPU Usage

Object:	Identifiers:	Attributes:	Datapoints:
Node	Node UUID	Node IP Node Name Node OS	Kernel Boot Time Kernel Context Switches (per sec) Kernel Entropy Available Kernel Interrupts (per sec) Kernel Processes Forked (per sec) Memory Active Memory Available Total Memory Available Memory Buffered Memory Cached Memory Commit Limit Memory Committed As Memory Dirty Memory Free Memory High Free Memory High Total Memory Huge Page Size Memory Huge Pages Free Memory Huge Pages Total Memory Low Free Memory Low Total Memory Mapped Memory Page Tables Memory Shared Memory Slab Memory Swap Cached Memory Swap Free Memory Swap Total Memory Total Memory Used Total Memory Used Memory Vmalloc Chunk Memory Vmalloc Total Memory Vmalloc Used Memory Wired Memory Writeback Total Memory Writeback Tmp Memory Cache Faults Memory Demand Zero Faults Memory Page Faults Memory Pages Memory Nonpaged Memory Paged Memory Cache Core Memory Standby Cache Normal Memory Standby Cache Reserve Memory Transition Faults Processes Blocked Processes Dead

Object:	Identifiers:	Attributes:	Datapoints:
Node Network	Network Interface Node UUID	Node Name Node IP Node OS	Bytes Received Bytes Sent Packets Outbound Discarded Packets Outbound Errors Packets Received Discarded Packets Received Errors Packets Received Packets Sent

Setup

Setup and Troubleshooting information can be found on the [Configuring an Agent](#) page.

MacOS Memory Usage

Cloud Insights (via Telegraf) and macOS report different numbers for memory usage. Both Telegraf and the Mac activity monitor use metrics gathered from `vm_stat`, however the total memory usage is calculated differently for each.

Telegraf calculates *Memory Used Total* as follows:

$$\text{Memory Used Total} = \text{Memory Total} - \text{Memory Available Total}$$

Where *Memory Available Total* is derived from the sum of "Pages free" and "Pages inactive" in `vm_stat`.

The Mac activity monitor, on the other hand, calculates Memory Used as follows:

$$\text{Memory Used} = \text{App Memory} + \text{Wired Memory} + \text{Compressed}$$

Where:

- *App Memory* is derived from the difference between "Anonymous pages" and "Pages purgeable" in `vm_stat`,
- *Wired Memory* is derived from "Pages wired down" in `vm_stat`, and
- *Compressed* is derived from "Pages occupied by compressor" in `vm_stat`.

ActiveMQ Data Collector

Cloud Insights uses this data collector to gather metrics from ActiveMQ.

Installation

1. From **Admin > Data Collectors**, click **+Data Collector**. Under **Services**, choose ActiveMQ.

Select the Operating System or Platform on which the Telegraf agent is installed.

2. If you haven't already installed an Agent for collection, or you wish to install an Agent for a different Operating System or Platform, click *Show Instructions* to expand the [Agent installation](#) instructions.
3. Select the Agent Access Key for use with this data collector. You can add a new Agent Access Key by clicking the **+ Agent Access Key** button. Best practice: Use a different Agent Access Key only when you want to group data collectors, for example, by OS/Platform.
4. Follow the configuration steps to configure the data collector. The instructions vary depending on the type of Operating System or Platform you are using to collect data.



ActiveMQ Configuration

Gathers ActiveMQ metrics.

What Operating System or Platform Are You Using?

Need Help?

Windows



Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)



+ Agent Access Key

*Please ensure that you have a Telegraf Agent in your environment before configuring. [Show Instructions](#)

Follow Configuration Steps

Need Help?

- 1 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-activemq.conf file.

```
[[inputs.activemq]]  
## Required ActiveMQ Endpoint, port  
## USER-ACTION: Provide address of ActiveMQ, HTTP port for ActiveMQ  
server = "<INSERT_ACTIVEMQ_ADDRESS>"  
port = <INSERT_ACTIVEMQ_PORT>
```



- 2 Replace <INSERT_ACTIVEMQ_ADDRESS> with the applicable ActiveMQ server address. Please specify a real machine address, and refrain from using a loopback address.
- 3 Replace <INSERT_ACTIVEMQ_PORT> with the applicable ActiveMQ server HTTP port.
- 4 Replace <INSERT_ACTIVEMQ_USERNAME> and <INSERT_ACTIVEMQ_PASSWORD> with the applicable ActiveMQ credentials.
- 5 Modify 'webadmin' if needed (if ActiveMQ server changes web admin root path).
- 6 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 7 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```



Setup

Information may be found in the [ActiveMQ documentation](#)

Objects and Counters

The following objects and their counters are collected:

Object:	Identifiers:	Attributes:	Datapoints:
ActiveMQ Queue	Namespace Queue Port Server	Node Name Node IP Node UUID	Consumer Count Dequeue Count Enqueue Count Queue Size
ActiveMQ Subscriber	Client ID Connection ID Port Server Namespace	Is Active Destination Node Name Node IP Node UUID Node OS Selector Subscription	Dequeue Count Dispatched Count Dispatched Queue Size Enqueue Count Pending Queue Size
ActiveMQ Topic	Topic Port Server Namespace	Node Name Node IP Node UUID Node OS	Consumer Count Dequeue Count Enqueue Count Size

Troubleshooting

Additional information may be found from the [Support](#) page.

Apache Data Collector

This data collector allows collection of data from Apache servers in your environment.

Pre-requisites

- You must have your Apache HTTP Server set up and properly running
- You must have sudo or administrator permissions on your agent host/VM
- Typically, the Apache *mod_status* module is configured to expose a page at the '/server-status?auto' location of the Apache server. The *ExtendedStatus* option must be enabled in order to collect all available fields. For information about how to configure your server, see the Apache module documentation:
https://httpd.apache.org/docs/2.4/mod/mod_status.html#enable

Installation

1. From **Admin > Data Collectors**, click **+Data Collector**. Under **Services**, choose Apache.
Select the Operating System or Platform on which the Telegraf agent is installed.
2. If you haven't already installed an Agent for collection, or you wish to install an Agent for a different Operating System or Platform, click *Show Instructions* to expand the **Agent installation** instructions.
3. Select the Agent Access Key for use with this data collector. You can add a new Agent Access Key by clicking the **+ Agent Access Key** button. Best practice: Use a different Agent Access Key only when you want to group data collectors, for example, by OS/Platform.

4. Follow the configuration steps to configure the data collector. The instructions vary depending on the type of Operating System or Platform you are using to collect data.



Apache Configuration

Gathers Apache metrics.

What Operating System or Platform Are You Using?

Ubuntu & Debian

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in your environment before configuring. [Show Instructions](#)

Follow Configuration Steps

1 Ensure that the Apache HTTP Server system you're going to gather metrics on has the 'mod_status' module enabled and exposed. For details refer to the following document.

2 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-apache.conf file.

```
[[inputs.apache]]  
## An array of URLs to gather from, must be directed at the machine  
## readable version of the mod_status page including the auto query string.  
## USER-ACTION: Provide address of apache server, port for apache server, confirm path for  
server-status.  
## Example: [[inputs.apache]] urls = ["http://192.168.1.10:80/server-status"]
```

3 Replace <INSERT_APACHE_ADDRESS> with the applicable Apache server address. Please specify a real machine address, and refrain from using a loopback address.

4 Replace <INSERT_APACHE_PORT> with the applicable Apache server port.

5 Modify the '/server-status' path in accordance to the Apache server configuration.

6 Restart the Telegraf service.

```
systemctl restart telegraf
```

Setup

Telegraf's plugin for Apache's HTTP Server relies on the 'mod_status' module to be enabled. When this is enabled, Apache's HTTP Server will expose an HTML endpoint that can be viewed on your browser or scraped for extraction of status of all Apache's HTTP Server configuration.

Compatibility:

Configuration was developed against Apache's HTTP Server version 2.4.38.

Enabling mod_status:

Enabling and exposing the 'mod_status' modules involves two steps:

- Enabling module
- Exposing stats from module

Enabling module:

The loading of modules is controlled by the config file under '/usr/local/apache/conf/httpd.conf'. Edit the config file and uncomment the following lines:

```
LoadModule status_module modules/mod_status.so
```

```
Include conf/extra/httpd-info.conf
```

Exposing stats from module:

The exposing of 'mod_status' is controlled by the config file under '/usr/local/apache2/conf/extra/httpd-info.conf'. Make sure you have the following in that configuration file (at least, other directives will be there):

```
# Allow server status reports generated by mod_status,
# with the URL of http://servername/server-status
<Location /server-status>
    SetHandler server-status
</Location>

#
# ExtendedStatus controls whether Apache will generate "full" status
# information (ExtendedStatus On) or just basic information
(ExtendedStatus
# Off) when the "server-status" handler is called. The default is Off.
#
ExtendedStatus On
```

For detailed instructions on the 'mod_status' module, see the [Apache documentation](#)

Objects and Counters

The following objects and their counters are collected:

Object:	Identifiers:	Attributes:	Datapoints:
Apache	Namespace Server	Node IP Node Name Port Parent Server Config Generation Parent Server MPM Generation Server Uptime Is Stopping	Busy Workers Bytes per Request Bytes per Second CPU Children System CPU Children User CPU Load CPU System CPU User Asynchronous Connections Closing Asynchronous Connections Keep Alive Asynchronous Connections Writing Connections Total Duration per Request Idle Workers Load Average (last 1m) Load Average (last 15m) Load Average (last 5m) Processes Requests per Second Total Accesses Total Duration Total KBytes Scoreboard Closing Scoreboard DNS Lookups Scoreboard Finishing Scoreboard Idle Cleanup Scoreboard Keep Alive Scoreboard Logging Scoreboard Open Scoreboard Reading Scoreboard Sending Scoreboard Starting Scoreboard Waiting

Troubleshooting

Additional information may be found from the [Support](#) page.

Consul Data Collector

Cloud Insights uses this data collector to gather metrics from Consul.

Installation

- From **Admin > Data Collectors**, click **+Data Collector**. Under **Services**, choose Consul.

If you haven't configured an Agent for collection, you are prompted to [install an agent](#) in your environment.

If you have an agent already configured, select the appropriate Operating System or Platform and click **Continue**.

2. Follow the instructions in the Consul Configuration screen to configure the data collector. The instructions vary depending on the type of Operating System or Platform you are using to collect data.

Setup

Information may be found in the [Consul documentation](#).

Objects and Counters for consul

The following objects and their counters are collected:

Object:	Identifiers:	Attributes:	Datapoints:
Consul	Namespace Check ID Service Node	Node IP Node OS Node UUID Node Name Service Name Check Name Service ID Status	Critical Passing Warning

Troubleshooting

Additional information may be found from the [Support](#) page.

Couchbase Data Collector

Cloud Insights uses this data collector to gather metrics from Couchbase.

Installation

1. From **Admin > Data Collectors**, click **+Data Collector**. Under **Services**, choose Couchbase.
Select the Operating System or Platform on which the Telegraf agent is installed.
2. If you haven't already installed an Agent for collection, or you wish to install an Agent for a different Operating System or Platform, click *Show Instructions* to expand the [Agent installation](#) instructions.
3. Select the Agent Access Key for use with this data collector. You can add a new Agent Access Key by clicking the **+ Agent Access Key** button. Best practice: Use a different Agent Access Key only when you want to group data collectors, for example, by OS/Platform.
4. Follow the configuration steps to configure the data collector. The instructions vary depending on the type of Operating System or Platform you are using to collect data.



Couchbase

Couchbase Configuration

Gathers Couchbase metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows



Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)



[+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in your environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-couchbase.conf file.

```
## Read metrics from one or many couchbase clusters
[[inputs.couchbase]]
  ## specify servers via a url matching:
  ## [protocol://[:password]@address[:port]
  ## e.g.
```



- 2 Replace <INSERT_USERNAME> and <INSERT_PASSWORD> with couchbase server account credentials.

- 3 Replace <INSERT_COUCHBASE_ADDRESS> with the applicable Couchbase address. Please specify a real machine address, and refrain from using a loopback address.

- 4 Replace <INSERT_COUCHBASE_PORT> with the applicable Couchbase port.

- 5 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```



Setup

Information may be found in the [Couchbase documentation](#).

Objects and Counters

The following objects and their counters are collected:

Object:	Identifiers:	Attributes:	Datapoints:
Couchbase Node	Namespace Cluster Couchbase Node Hostname	Node Name Node IP	Memory Free Memory Total
Couchbase Bucket	Namespace Bucket Cluster	Node Name Node IP	Data Used Data Fetches Disk Used Item Count Memory Used Operations Per Second Quota Used

Troubleshooting

Additional information may be found from the [Support](#) page.

CouchDB Data Collector

Cloud Insights uses this data collector to gather metrics from CouchDB.

Installation

- From **Admin > Data Collectors**, click **+Data Collector**. Under **Services**, choose CouchDB.
Select the Operating System or Platform on which the Telegraf agent is installed.
- If you haven't already installed an Agent for collection, or you wish to install an Agent for a different Operating System or Platform, click *Show Instructions* to expand the [Agent installation](#) instructions.
- Select the Agent Access Key for use with this data collector. You can add a new Agent Access Key by clicking the **+ Agent Access Key** button. Best practice: Use a different Agent Access Key only when you want to group data collectors, for example, by OS/Platform.
- Follow the configuration steps to configure the data collector. The instructions vary depending on the type of Operating System or Platform you are using to collect data.



CouchDB Configuration

Gathers CouchDB metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

RHEL & CentOS

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

[+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in your environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-couchdb.conf file.

```
## Read CouchDB Stats from one or more servers
[[inputs.couchdb]]
    ## Works with CouchDB stats endpoints out of the box
    ## Multiple Hosts from which to read CouchDB stats:
    ## USER-ACTION: Provide comma-separated list of couchdb IP(s) and port(s).
    ## Example: [[inputs.couchdb]]
```

- 2 Replace <INSERT_COUCHDB_ADDRESS> with the applicable CouchDB address. Please specify a real machine address, and refrain from using a loopback address.

- 3 Replace <INSERT_COUCHDB_PORT> with the applicable CouchDB port.

- 4 Modify the URL if CouchDB monitoring is exposed at different path

- 5 Restart the Telegraf service.

```
systemctl restart telegraf
```

Setup

Information may be found in the [CouchDB documentation](#).

Objects and Counters

The following objects and their counters are collected:

Object:	Identifiers:	Attributes:	Datapoints:
CouchDB	Namespace Server	Node Name Node IP	Authentication Cache Hits Authentication Cache Miss Database Reads Database Writes Databases Open Open OS Files Max Request Time Min Request Time Httpd Request Methods Copy Httpd Request Methods Delete Httpd Request Methods Get Httpd Request Methods Head Httpd Request Methods Post Httpd Request Methods Put Status Codes 200 Status Codes 201 Status Codes 202 Status Codes 301 Status Codes 304 Status Codes 400 Status Codes 401 Status Codes 403 Status Codes 404 Status Codes 405 Status Codes 409 Status Codes 412 Status Codes 500

Troubleshooting

Additional information may be found from the [Support](#) page.

Docker Data Collector

Cloud Insights uses this data collector to gather metrics from Docker.

Installation

- From **Admin > Data Collectors**, click **+Data Collector**. Under **Services**, choose Docker.

If you haven't configured an Agent for collection, you are prompted to [install an agent](#) in your environment.

If you have an agent already configured, select the appropriate Operating System or Platform and click **Continue**.

2. Follow the instructions in the Docker Configuration screen to configure the data collector. The instructions vary depending on the type of Operating System or Platform you are using to collect data.

The screenshot shows the 'Docker Configuration' screen for a 'CloudInsights' service. It includes a 'docker' logo, a brief description ('Gathers Docker metrics.'), and a dropdown menu for 'What Operating System or Platform Are You Using?' set to 'RHEL & CentOS'. A note says 'Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)'. A blue button '+ Agent Access Key' is visible. Below, a note states: '*Please ensure that you have a Telegraf Agent in your environment before configuring. Show Instructions'. The 'Follow Configuration Steps' section lists four numbered steps: 1. Copy contents into a .conf file, showing a code block for the [inputs.docker] configuration. 2. Replace <INSERT_DOCKER_ENDPOINT>. 3. Modify 'Namespace'. 4. Restart the Telegraf service, showing a terminal command 'systemctl restart telegraf'. Each step has a 'Need Help?' link.

Docker Configuration
Gathers Docker metrics.

What Operating System or Platform Are You Using?

RHEL & CentOS

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in your environment before configuring. [Show Instructions](#)

Follow Configuration Steps

1 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-docker.conf file.

```
[[inputs.docker]]  
## Docker Endpoint  
## To use TCP, set endpoint = "tcp://[ip]:[port]". By default, Docker uses port 2375 for  
unencrypted and 2376 for encrypted  
## To use environment variables (ie, docker-machine), set endpoint = "ENV"
```

2 Replace <INSERT_DOCKER_ENDPOINT> with the applicable Docker endpoint.

3 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).

4 Restart the Telegraf service.

```
systemctl restart telegraf
```

Setup

The Telegraf input plugin for Docker collects metrics through a specified UNIX socket or a TCP endpoint.

Compatibility

Configuration was developed against Docker version 1.12.6.

Setting Up

Accessing Docker through a UNIX socket

If the Telegraf agent is running on baremetal, add the telegraf Unix user to the docker Unix group by running the following:

```
sudo usermod -aG docker telegraf
```

If the Telegraf agent is running within a Kubernetes pod, expose the Docker Unix socket by mapping the socket into the pod as a volume and then mounting that volume to /var/run/docker.sock. For example, add the following to the PodSpec:

```
volumes:  
...  
- name: docker-sock  
hostPath:  
path: /var/run/docker.sock  
type: File
```

Then, add the following to the Container:

```
volumeMounts:  
...  
- name: docker-sock  
mountPath: /var/run/docker.sock
```

Note that the Cloud Insights installer provided for the Kubernetes platform takes care of this mapping automatically.

Access Docker through a TCP endpoint

By default, Docker uses port 2375 for unencrypted access and port 2376 for encrypted access.

Objects and Counters

The following objects and their counters are collected:

Object:	Identifiers:	Attributes:	Datapoints:
Docker Engine	Namespace Docker Engine	Node Name Node IP Node UUID Node OS Kubernetes Cluster Docker Version Unit	Memory Containers Containers Paused Containers Running Containers Stopped CPUs Go Routines Images Listener Events Used File Descriptors Data Available Data Total Data Used Metadata Available Metadata Total Metadata Used Pool Blocksize

Object:	Identifiers:	Attributes:	Datapoints:
Docker Container	Namespace Container Name Docker Engine	Kubernetes Container Hash Kubernetes Container Ports Kubernetes Container Restart Count Kubernetes Container Termination Message Path Kubernetes Container Termination Message Policy Kubernetes Pod Termination Grace Period Container Image Container Status Container Version Node Name Kubernetes Container Log Path Kubernetes Container Name Kubernetes Docker Type Kubernetes Pod Name Kubernetes Pod Namespace Kubernetes Pod UID Kubernetes Sandbox ID Node IP Node UUID Docker Version Kubernetes IO Config Seen Kubernetes IO Config Source OpenShift IO SCC Kubernetes Description Kubernetes Display Name OpenShift Tags Kompose Service Pod Template Hash Controller Revision Hash Pod Template Generation License Schema Build Date Schema License Schema Name Schema URL Schema VCS URL Schema Vendor Schema Version Schema Schema Version Maintainer Customer Pod	Memory Active Anonymous Memory Active File Memory Cache Memory Hierarchical Limit Memory Inactive Anonymous Memory Inactive File Memory Limit Memory Mapped File Memory Max Usage Memory Page Fault Memory Page Major Fault Memory Paged In Memory Paged Out Memory Resident Set Size Memory Resident Set Size Huge Memory Total Active Anonymous Memory Total Active File Memory Total Cache Memory Total Inactive Anonymous Memory Total Inactive File Memory Total Mapped File Memory Total Page Fault Memory Total Page Major Fault Memory Total Paged In Memory Total Paged Out Memory Total Resident Set Size Memory Total Resident Set Size Huge Memory Total Unevictable Memory Unevictable Memory Usage Memory Usage Percent Exit Code OOM Killed PID Started At Failing Streak

Object:	Identifiers:	Attributes:	Datapoints:
Docker Container Block IO	Namespace Container Name Device Docker Engine	Kubernetes Container Hash Kubernetes Container Ports Kubernetes Container Restart Count Kubernetes Container Termination Message Path Kubernetes Container Termination Message Policy Kubernetes Pod Termination Grace Period Container Image Container Status Container Version Node Name Kubernetes Container Log Path Kubernetes Container Name Kubernetes Docker Type Kubernetes Pod Name Kubernetes Pod Namespace Kubernetes Pod UID Kubernetes Sandbox ID Node IP Node UUID Docker Version Kubernetes Config Seen Kubernetes Config Source OpenShift SCC Kubernetes Description Kubernetes Display Name OpenShift Tags Schema Schema Version Pod Template Hash Controller Revision Hash Pod Template Generation Kompose Service Schema Build Date Schema License Schema Name Schema Vendor Customer Pod Kubernetes StatefulSet Pod Name Tenant Webconsole Build Date License Vendor	IO Service Bytes Recursive Async IO Service Bytes Recursive Read IO Service Bytes Recursive Sync IO Service Bytes Recursive Total IO Service Bytes Recursive Write IO Serviced Recursive Async IO Serviced Recursive Read IO Serviced Recursive Sync IO Serviced Recursive Total IO Serviced Recursive Write

Object:	Identifiers:	Attributes:	Datapoints:
Docker Container Network	Namespace Container Name Network Docker Engine	Container Image Container Status Container Version Node Name Node IP Node UUID Node OS K8s Cluster Docker Version Container ID	RX Dropped RX Bytes RX Errors RX Packets TX Dropped TX Bytes TX Errors TX Packets

Object:	Identifiers:	Attributes:	Datapoints:
Docker Container CPU	Namespace Container Name CPU Docker Engine	Kubernetes Container Hash Kubernetes Container Ports Kubernetes Container Restart Count Kubernetes Container Termination Message Path Kubernetes Container Termination Message Policy Kubernetes Pod Termination Grace Period Kubernetes Config Seen Kubernetes Config Source OpenShift SCC Container Image Container Status Container Version Node Name Kubernetes Container Log Path Kubernetes Container name Kubernetes Docker Type Kubernetes Pod Name Kubernetes Pod Namespace Kubernetes Pod UID Kubernetes Sandbox ID Node IP Node UUID Node OS Kubernetes Cluster Docker Version Kubernetes Description Kubernetes Display Name OpenShift Tags Schema Version Pod Template Hash Controller Revision Hash Pod Template Generation Kompose Service Schema Build Date Schema License Schema Name Schema Vendor Customer Pod Kubernetes StatefulSet Pod Name Tenant Webconsole Build Date	Throttling Periods Throttling Throttled Periods Throttling Throttled Time Usage In Kernel Mode Usage In User Mode Usage Percent Usage System Usage Total

Troubleshooting

Problem:	Try this:
I do not see my Docker metrics in Cloud Insights after following the instructions on the configuration page.	<p>Check the Telegraf agent logs to see if it reports the following error:</p> <p>E! Error in plugin [inputs.docker]: Got permission denied while trying to connect to the Docker daemon socket</p> <p>If it does, take the necessary steps to provide the Telegraf agent access to the Docker Unix socket as specified above.</p>

Additional information may be found from the [Support](#) page.

Elasticsearch Data Collector

Cloud Insights uses this data collector to gather metrics from Elasticsearch.

1. From **Admin > Data Collectors**, click **+Data Collector**. Under **Services**, choose Elasticsearch.
Select the Operating System or Platform on which the Telegraf agent is installed.
2. If you haven't already installed an Agent for collection, or you wish to install an Agent for a different Operating System or Platform, click *Show Instructions* to expand the [Agent installation](#) instructions.
3. Select the Agent Access Key for use with this data collector. You can add a new Agent Access Key by clicking the **+ Agent Access Key** button. Best practice: Use a different Agent Access Key only when you want to group data collectors, for example, by OS/Platform.
4. Follow the configuration steps to configure the data collector. The instructions vary depending on the type of Operating System or Platform you are using to collect data.



Elasticsearch Configuration

Gathers Elasticsearch metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Ubuntu & Debian



Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)



[+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in your environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-elasticsearch.conf file.

```
[[inputs.elasticsearch]]  
## USER-ACTION: Provide comma-separated list of Elasticsearch servers.  
## Note that for scenarios in which metrics from multiple Elasticsearch clusters are being  
## sent to Cloud Insights, the Elasticsearch cluster names must be unique.  
## Please specify actual machine IP address, and refrain from using a loopback address
```



- 2 Replace <INSERT_ESPRESSO_ADDRESS> with the applicable Elasticsearch address. Please specify a real machine address, and refrain from using a loopback address.

- 3 Replace <INSERT_ESPRESSO_PORT> with the applicable Elasticsearch port.

- 4 Restart the Telegraf service.

```
systemctl restart telegraf
```



Setup

Information may be found in the [Elasticsearch documentation](#).

Objects and Counters

The following objects and their counters are collected:

Object:	Identifiers:	Attributes:	Datapoints:
Elasticsearch Cluster	Namespace Cluster	Node IP Node Name Cluster Status	Master Node Count Total Node Count Filesystem Data Available (bytes) Filesystem Data Free (bytes) Filesystem Data Total (bytes) JVM Threads OS Allocated Processors OS Available Processors OS Mem Free (bytes) OS Mem Free OS Mem Total (bytes) OS Mem Used (bytes) OS Mem Used Process CPU Indices Completion Size (bytes) Indices Count Indices Docs Count Indices Docs Deleted Indices Field Data Evictions Indices Field Data Memory Size (bytes) Indices Query Cache Count Indices Cache Size Indices Segments Count Indices Segments Doc Values Memory (bytes) Indices Shards Index Primaries Avg Indices Shards Index Primaries Max Indices Shards Index Primaries Min Indices Shards Index Replication Avg Indices Shards Index Replication Max Indices Shards Index Replication Min Indices Shards Avg Indices Shards Max Indices Shards Primaries Indices Shards Replication Indices Shards Total Indices Store Size (bytes)

Object:	Identifiers:	Attributes:	Datapoints:
Elasticsearch Node	Namespace Cluster ES Node ID ES Node IP ES Node	Zone ID	Machine Learning Enabled Machine Learning Memory Machine Learning Max Open Jobs X-Pack Installed Breakers Accounting Estimated Size (bytes) Breakers Accounting Limit Size (bytes) Breakers Accounting Overhead Breakers Accounting Tripped Breakers Field Data Estimated Size (bytes) Breakers Field Data Limit Size (bytes) Breakers Field Data Overhead Breakers Field Data Tripped Breakers In-Flight Sstimated Size (bytes) Breakers In-Flight Limit Size (bytes) Breakers In-Flight Overhead Breakers In-Flight Tripped Breakers Parent Estimated Size (bytes) Breakers Parent Limit Size (bytes) Breakers Parent Overhead Breakers Parent Tripped Breakers Request Estimated Size (bytes) Breakers Request Limit Size (bytes) Breakers Request Overhead Breakers Request Tripped Filesystem Data Available (bytes) Filesystem Data Free (bytes) Filesystem Data Total (bytes) Filesystem IO Stats Devices Ops Filesystem IO Stats Devices Read (kb)

Troubleshooting

Additional information may be found from the [Support](#) page.

Flink Data Collector

Cloud Insights uses this data collector to gather metrics from Flink.

Installation

1. From **Admin > Data Collectors**, click **+Data Collector**. Under **Services**, choose Flink.
Select the Operating System or Platform on which the Telegraf agent is installed.
2. If you haven't already installed an Agent for collection, or you wish to install an Agent for a different Operating System or Platform, click *Show Instructions* to expand the [Agent installation](#) instructions.
3. Select the Agent Access Key for use with this data collector. You can add a new Agent Access Key by clicking the **+ Agent Access Key** button. Best practice: Use a different Agent Access Key only when you want to group data collectors, for example, by OS/Platform.
4. Follow the configuration steps to configure the data collector. The instructions vary depending on the type of Operating System or Platform you are using to collect data.



Flink Configuration

Gathers Flink metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

[+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in your environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Install Jolokia on your Flink JobManager(s) and Flink Task Manager(s). For details refer to the following document.
[Install Jolokia](#)
- 2 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-flink.conf file.

```
## #####  
## JobManager  
## #####  
[[inputs.jolokia2_agent]]  
  ## USER-ACTION: Provide address(es) of flink Job Manager(s), port for jolokia, add one URL  
  ## Example: [[{"url": "http://192.168.1.10:8081"}]]
```
- 3 Replace <INSERT_FLINK_JOBMANAGER_ADDRESS> with the applicable Flink Job Manager address(es). Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT_FLINK_TASKMANAGER_ADDRESS> with the applicable Flink Task Manager address(es). Please specify a real machine address, and refrain from using a loopback address.
- 5 Replace <INSERT_JOLOKIA_PORT> with the applicable jolokia port.
- 6 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 7 Modify 'Cluster' if needed for Flink cluster designation.
- 8 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Setup

A full Flink deployment involves the following components:

JobManager: The Flink primary system. Coordinates a series of TaskManagers. In a High Availability setup, system will have more than one JobManager.

TaskManager: This is where Flink operators are executed.

The Flink plugin is based on the telegraf's Jolokia plugin. As such as a requirement to gather info from all Flink components, JMX needs to be configured and exposed via Jolokia on all components.

Compatibility

Configuration was developed against Flink version 1.7.0.

Setting Up

Jolokia Agent Jar

For all individual components, a version the Jolokia agent jar file must be downloaded. The version tested against was [Jolokia agent 1.6.0](#).

Instructions below assume that downloaded jar file (jolokia-jvm-1.6.0-agent.jar) is placed under location '/opt/flink/lib/'.

JobManager

To configure JobManager to expose the Jolokia API, you can setup the following environment variable on your nodes then restart the JobManager:

```
export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0"
```

You can choose a different port for Jolokia (8778). If you have an internal IP to lock Jolokia onto you can replace the "catch all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from the telegraf plugin.

TaskManager

To configure TaskManager(s) to expose the Jolokia API, you can setup the following environment variable on your nodes then restart the TaskManager:

```
export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0"
```

You can choose a different port for Jolokia (8778). If you have an internal IP to lock Jolokia onto you can replace the "catch all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from the telegraf plugin.

Objects and Counters

The following objects and their counters are collected:

Object:	Identifiers:	Attributes:	Datapoints:
Flink Task Manager	Cluster Namespace Server	Node Name Task Manager ID Node IP	Network Available Memory Segments Network Total Memory Segments Garbage Collection PS MarkSweep Count Garbage Collection PS MarkSweep Time Garbage Collection PS Scavenge Count Garbage Collection PS Scavenge Time Heap Memory Committed Heap Memory Init Heap Memory Max Heap Memory Used Thread Count Daemon Thread Count Peak Thread Count Thread Count Total Started
Flink Job	Cluster Namespace server Job ID	Node Name Job Name Node IP Last Checkpoint External Path Restarting Time	Downtime Full Restarts Last Checkpoint Alignment Buffered Last Checkpoint Duration Last Checkpoint Size Number of Completed Checkpoints Number of Failed Checkpoints Number of in Progress Checkpoints Number of Checkpoints Uptime

Object:	Identifiers:	Attributes:	Datapoints:
Flink Job Manager	Cluster Namespace Server	Node Name Node IP	Garbage Collection PS MarkSweep Count Garbage Collection PS MarkSweep Time Garbage Collection PS Scavenge Count Garbage Collection PS Scavenge Time Heap Memory Committed Heap Memory Init Heap Memory Max Heap Memory Used Number Registered Task Managers Number Running Jobs Task Slots Available Task Slots Total Thread Count Daemon Thread Count Peak Thread Count Thread Count Total Started

Object:	Identifiers:	Attributes:	Datapoints:
Flink Task	Cluster Namespace Job ID Task ID	Server Node Name Job Name Sub Task Index Task Attempt ID Task Attempt Number Task Name Task Manager ID Node IP Current Input Watermark	Buffers In Pool Usage Buffers In Queue Length Buffers Out Pool Usage Buffers Out Queue Length Number Buffers In Local Number Buffers In Local Per Second Count Number Buffers in Local Per Second Rate Number Buffers In Remote Number Buffers In Remote Per Second Count Number Buffers In Remote Per Second Rate Number Buffers Out Number Buffers Out Per Second Count Number Buffers Out Per Second Rate Number Bytes In Local Number Bytes In Local Per Second Count Number Bytes In Local Per Second Rate Number Bytes In Remote Number Bytes In Remote Per Second Count Number Bytes In Remote Per Second Rate Number Bytes Out Number Bytes Out Per Second Count Number Bytes Out Per Second Rate Number Records In Number Records In Per Second Count Number Records In Per Second Rate Number Records Out Number Records Out Per Second Count Number Records Out Per Second Rate

Object:	Identifiers:	Attributes:	Datapoints:
Flink Task Operator	Cluster Namespace Job ID Operator ID Task ID	Server Node Name Job Name Operator Name Sub Task Index Task Attempt ID Task Attempt Number Task Name Task Manager ID Node IP	Current Input Watermark Current Output Watermark Number Records In Number Records In Per Second Count Number Records In Per Second Rate Number Records Out Number Records Out Per Second Count Number Records Out Per Second Rate Number Late Records Dropped Assigned Partitions Bytes Consumed Rate Commit Latency Avg Commit Latency Max Commit Rate Commits Failed Commits Succeeded Connection Close Rate Connection Count Connection Creation Rate Count Fetch Latency Avg Fetch Latency Max Fetch Rate Fetch Size Avg Fetch Size Max Fetch Throttle Time Avg Fetch Throttle Time Max Heartbeat Rate Incoming Byte Rate IO Ratio IO Time Avg (ns) IO Wait Ratio IO Wait Time Avg (ns) Join Rate Join Time Avg Last Heartbeat Ago Network IO Rate Outgoing Byte Rate Records Consumed Rate Records Lag Max Records per Request Avg Request Rate Request Size Avg Request Size Max Response Rate Select Rate Sync Rate Sync Time Avg Heartbeat Response Time

Troubleshooting

Additional information may be found from the [Support](#) page.

Hadoop Data Collector

Cloud Insights uses this data collector to gather metrics from Hadoop.

Installation

1. From **Admin > Data Collectors**, click **+Data Collector**. Under **Services**, choose Hadoop.
Select the Operating System or Platform on which the Telegraf agent is installed.
2. If you haven't already installed an Agent for collection, or you wish to install an Agent for a different Operating System or Platform, click *Show Instructions* to expand the [Agent installation](#) instructions.
3. Select the Agent Access Key for use with this data collector. You can add a new Agent Access Key by clicking the **+ Agent Access Key** button. Best practice: Use a different Agent Access Key only when you want to group data collectors, for example, by OS/Platform.
4. Follow the configuration steps to configure the data collector. The instructions vary depending on the type of Operating System or Platform you are using to collect data.

The screenshot shows the 'Hadoop Configuration' page. At the top, there's a logo for 'hadoop' and the text 'Hadoop Configuration' followed by a subtitle 'Gathers Hadoop metrics.' Below this, there's a section titled 'What Operating System or Platform Are You Using?' with a dropdown menu set to 'Ubuntu & Debian'. To the right of the dropdown is a 'Need Help?' link. Further down, there's a section titled 'Select existing Agent Access Key or create a new one' with a dropdown menu showing 'Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)' and a blue button labeled '+ Agent Access Key'. At the bottom of the page, a note says '*Please ensure that you have a Telegraf Agent in your environment before configuring' followed by a 'Show Instructions' link.

Follow Configuration Steps

Need Help?

- 1 Install Jolokia on your Hadoop NameNode, Secondary NameNode, DataNode(s), ResourceManager, NodeManager(s) and JobHistoryServer. For details refer to the following document.
- 2 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-hadoop.conf file.

```
#####
# NAMENODE      #
#####
[[inputs.jolokia2_agent]]
## USER-ACTION: Provide address(es) of Hadoop NameNode, port for jolokia
##
```
- 3 Replace <INSERT_HADOOP_NAMENODE_ADDRESS> with the applicable Hadoop NameNode address. Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT_JOLOKIA_PORT> with the NameNode's assigned Jolokia port.
- 4 Replace <INSERT_HADOOP_SECONDARYNAMENODE_ADDRESS> with the applicable Hadoop Secondary NameNode address. Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT_JOLOKIA_PORT> with the Secondary NameNode's assigned Jolokia port.
- 5 Replace <INSERT_HADOOP_DATANODE_ADDRESS> with the applicable Hadoop DataNode address(es). Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT_JOLOKIA_PORT> with the DataNode's assigned Jolokia port.
- 6 Replace <INSERT_HADOOP_RESOURCEMANAGER_ADDRESS> with the applicable Hadoop ResourceManager address. Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT_JOLOKIA_PORT> with the ResourceManager's assigned Jolokia port.
- 7 Replace <INSERT_HADOOP_NODEMANAGER_ADDRESS> with the applicable Hadoop NodeManager address(es). Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT_JOLOKIA_PORT> with the NodeManager's assigned Jolokia port.
- 8 Replace <INSERT_HADOOP_JOBHISTORYSERVER_ADDRESS> with the applicable Hadoop Job History Server address. Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT_JOLOKIA_PORT> with the Job History Server's assigned Jolokia port.
- 9 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 10 Modify 'Cluster' if needed for Hadoop cluster designation.
- 11 Restart the Telegraf service.

```
systemctl restart telegraf
```

Setup

A full Hadoop deployment involves the following components:

- NameNode: The Hadoop Distributed File System (HDFS) primary system. Coordinates a series of DataNodes.

- Secondary NameNode: a warm failover for the main NameNode. In Hadoop the promotion to NameNode does not occur automatically. Secondary NameNode gathers information from NameNode to be ready to be promoted when needed.
- DataNode: Actual owner for data.
- ResourceManager: The compute primary system (Yarn). Coordinates a series of NodeManagers.
- NodeManager: The resource for compute. Actual location for running of applications.
- JobHistoryServer: Responsible for servicing all job history related requests.

The Hadoop plugin is based on the telegraf's Jolokia plugin. As such as a requirement to gather info from all Hadoop components, JMX needs to be configured and exposed via Jolokia on all components.

Compatibility

Configuration was developed against Hadoop version 2.9.2.

Setting Up

Jolokia Agent Jar

For all individual components, a version the Jolokia agent jar file must be downloaded. The version tested against was [Jolokia agent 1.6.0](#).

Instructions below assume that downloaded jar file (jolokia-jvm-1.6.0-agent.jar) is placed under location '/opt/hadoop/lib/'.

NameNode

To configure NameNode to expose the Jolokia API, you can setup the following in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export HADOOP_NAMENODE_OPTS="$HADOOP_NAMENODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7800,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8000
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.password"
```

You can choose a different port for JMX (8000 above) and Jolokia (7800). If you have an internal IP to lock Jolokia onto you can replace the "catch all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from the telegraf plugin. You can use the option '-Dcom.sun.management.jmxremote.authenticate=false' if you don't want to authenticate. Use at your own risk.

Secondary NameNode

To configure the Secondary NameNode to expose the Jolokia API, you can setup the following in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export HADOOP_SECONDARYNAMENODE_OPTS="$HADOOP_SECONDARYNAMENODE_OPTS  
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0  
-agent.jar=port=7802,host=0.0.0.0 -Dcom.sun.management.jmxremote  
-Dcom.sun.management.jmxremote.port=8002  
-Dcom.sun.management.jmxremote.ssl=false  
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p  
assword"
```

You can choose a different port for JMX (8002 above) and Jolokia (7802). If you have an internal IP to lock Jolokia onto you can replace the "catch all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from the telegraf plugin. You can use the option '
-Dcom.sun.management.jmxremote.authenticate=false' if you don't want to authenticate. Use at your own risk.

DataNode

To configure the DataNodes to expose the Jolokia API, you can setup the following in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export HADOOP_DATANODE_OPTS="$HADOOP_DATANODE_OPTS  
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0  
-agent.jar=port=7801,host=0.0.0.0 -Dcom.sun.management.jmxremote  
-Dcom.sun.management.jmxremote.port=8001  
-Dcom.sun.management.jmxremote.ssl=false  
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p  
assword"
```

You can choose a different port for JMX (8001 above) and Jolokia (7801). If you have an internal IP to lock Jolokia onto you can replace the "catch all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from the telegraf plugin. You can use the option '
-Dcom.sun.management.jmxremote.authenticate=false' if you don't want to authenticate. Use at your own risk.

ResourceManager

To configure the ResourceManager to expose the Jolokia API, you can setup the following in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export YARN_RESOURCEMANAGER_OPTS="$YARN_RESOURCEMANAGER_OPTS  
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0  
-agent.jar=port=7803,host=0.0.0.0 -Dcom.sun.management.jmxremote  
-Dcom.sun.management.jmxremote.port=8003  
-Dcom.sun.management.jmxremote.ssl=false  
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p  
assword"
```

You can choose a different port for JMX (8003 above) and Jolokia (7803). If you have an internal IP to lock Jolokia onto you can replace the "catch all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from the telegraf plugin. You can use the option '
-Dcom.sun.management.jmxremote.authenticate=false' if you don't want to authenticate. Use at your own risk.

NodeManager

To configure the NodeManagers to expose the Jolokia API, you can setup the following in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export YARN_NODEMANAGER_OPTS="$YARN_NODEMANAGER_OPTS  
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0  
-agent.jar=port=7804,host=0.0.0.0 -Dcom.sun.management.jmxremote  
-Dcom.sun.management.jmxremote.port=8004  
-Dcom.sun.management.jmxremote.ssl=false  
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p  
assword"
```

You can choose a different port for JMX (8004 above) and Jolokia (7804). If you have an internal IP to lock Jolokia onto you can replace the "catch all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from the telegraf plugin. You can use the option '
-Dcom.sun.management.jmxremote.authenticate=false' if you don't want to authenticate. Use at your own risk.

JobHistoryServer

To configure the JobHistoryServer to expose the Jolokia API, you can setup the following in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```

export HADOOP_JOB_HISTORYSERVER_OPTS="$HADOOP_JOB_HISTORYSERVER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7805,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8005
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"

```

You can choose a different port for JMX (8005 above) and Jolokia (7805). If you have an internal IP to lock Jolokia onto you can replace the "catch all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from the telegraf plugin. You can use the option '`-Dcom.sun.management.jmxremote.authenticate=false`' if you don't want to authenticate. Use at your own risk.

Objects and Counters

The following objects and their counters are collected:

Object:	Identifiers:	Attributes:	Datapoints:
Hadoop Secondary NameNode	Cluster Namespace Server	Node Name Node IP Compile Info Version	GC Count GC Copies Count GC Marks Sweep Compact Count GC Number Info Threshold Exceeded GC Number Warning Threshold Exceeded GC Time GC Copy Time GC Marks Sweep Compact Time GC Total Extra Sleep Time Logs Error Count Logs Fatal Count Logs Info Count Logs Warn Count Memory Heap Committed Memory Heap Max Memory Heap Used Memory Max Memory Non Heap Committed Memory Non Heap Max Memory Non Heap Used Threads Blocked Threads New Threads Runnable Threads Terminated Threads Timed Waiting Threads Waiting

Object:	Identifiers:	Attributes:	Datapoints:
Hadoop NodeManager	Cluster Namespace Server	Node Name Node IP	Containers Allocated Memory Allocate Memory Allocated Oportunistic Virtual Cores Allocated Oportunistic Virtual Cores Allocated Memory Available Virtual Cores Available Directories Bad Local Directories Bad Log Cache Size Before Clean Container Launch Duration Avg Time Container Launch Duration Number Of Operations Containers Completed Containers Failed Containers Inititing Containers Killed Containers Launched Containers Reiniting Containers Rolled Back on Failure Containers Running Disk Utilization Good Local Directories Disk Utilization Good Log Directories Bytes Deleted Private Bytes Deleted Public Containers Running Opportunistic Bytes Deleted Total Shuffle Connections Shuffle Output Bytes Shuffle Outputs Failed Shuffle Outputs Ok GC Count GC Copies Count GC Marks Sweep Compact Count GC Number Info Threshold Exceeded GC Number Warning Threshold Exceeded GC Time GC Copy Time GC Marks Sweep Compact Time GC Total Extra Sleep Time Logs Error Count Logs Fatal Count

Object:	Identifiers:	Attributes:	Datapoints:
Hadoop ResourceManager	Cluster Namespace Server	Node Name Node IP	ApplicationMaster Launch Delay Avg ApplicationMaster Launch Delay Number ApplicationMaster Register Delay Avg ApplicationMaster Register Delay Number NodeManager Active Number NodeManager Decommissioned Number NodeManager Decommissioning Number NodeManager Lost Number NodeManager Rebooted Number NodeManager Shutdown Number NodeManager Healthy Number NodeManager Memory Limit NodeManager Virtual Cores Limit Used Capacity Active Applications Active Users Aggregate Containers Allocated Aggregate Containers Preempted Aggregate Containers Released Aggregate Memory Seconds Preempted Aggregate Node Local Containers Allocated Aggregate Off Switch Containers Allocated Aggregate Ack Local Containers Allocated Aggregate Virtual Cores Seconds Preempted Containers Allocated Memory Allocated Virtual Cores Allocated Application Attempt First Container Allocation Delay Avg Time Application Attempt First Container Allocation Delay Number

Object:	Identifiers:	Attributes:	Datapoints:
Hadoop DataNode	Cluster Namespace Server	Node Name Node IP Cluster ID Version	Transceiver Count Transmits in Progress Cache Capacity Cache Used Capacity DFS Used Estimated Capacity Lost Total Last Volume Failure Rate Blocks Number Cached Blocks Number Failed to Cache Blocks Number Failed to Uncache Volumes Number Failed Capacity Remaining GC Count GC Copies Count GC Marks Sweep Compact Count GC Number Info Threshold Exceeded GC Number Warning Threshold Exceeded GC Time GC Copy Time GC Marks Sweep Compact Time GC Total Extra Sleep Time Logs Error Count Logs Fatal Count Logs Info Count Logs Warn Count Memory Heap Committed Memory Heap Max Memory Heap Used Memory Max Memory Non Heap Committed Memory Non Heap Max Memory Non Heap Used Threads Blocked Threads New Threads Runnable Threads Terminated Threads Timed Waiting Threads Waiting

Object:	Identifiers:	Attributes:	Datapoints:
Hadoop NameNode	Cluster Namespace Server	Node Name Node IP Transaction ID Last Written Time Since Last Loaded Edits HA State File System State Block Pool ID Cluster ID Compile Info Distinct Version Count Version	Block Capacity Blocks Total Capacity Total Capacity Used Capacity Used Non DFS Blocks Corrupt Estimated Capacity Lost Total Blocks Excess Heartbeats Expired Files Total File System Lock Queue Length Blocks Missing Blocks Missing Replication with Factor One Clients Active Data Nodes Dead Data Nodes Decommissioning Dead Data Nodes Decommissioning Live Data Nodes Decommissioning Encryption Zones Number Data Nodes Entering Maintenance Files Under Construction Data Nodes Dead in Maintenance Data Nodes Live in Maintenance Data Nodes Live Storages Stale Replication Pending Timeouts Data Node Message Pending Blocks Pending Deletion Blocks Pending Replication Blocks Misreplicated Postponed Blocks Scheduled Replication Snapshots Snapshottable Directories Data Nodes Stale Files Total Load Total Sync Count Total Transactions Since Last Checkpoint

Object:	Identifiers:	Attributes:	Datapoints:
Hadoop JobHistoryServer	Cluster Namespace Server	Node Name Node IP	GC Count GC Copies Count GC Marks Sweep Compact Count GC Number Info Threshold Exceeded GC Number Warning Threshold Exceeded GC Time GC Copy Time GC Marks Sweep Compact Time GC Total Extra Sleep Time Logs Error Count Logs Fatal Count Logs Info Count Logs Warn Count Memory Heap Committed Memory Heap Max Memory Heap Used Memory Max Memory Non Heap Committed Memory Non Heap Max Memory Non Heap Used Threads Blocked Threads New Threads Runnable Threads Terminated Threads Timed Waiting Threads Waiting

Troubleshooting

Additional information may be found from the [Support](#) page.

HAProxy Data Collector

Cloud Insights uses this data collector to gather metrics from HAProxy.

Installation

- From **Admin > Data Collectors**, click **+Data Collector**. Under **Services**, choose HAProxy.
 Select the Operating System or Platform on which the Telegraf agent is installed.
- If you haven't already installed an Agent for collection, or you wish to install an Agent for a different Operating System or Platform, click *Show Instructions* to expand the [Agent installation](#) instructions.
- Select the Agent Access Key for use with this data collector. You can add a new Agent Access Key by clicking the **+ Agent Access Key** button. Best practice: Use a different Agent Access Key only when you

want to group data collectors, for example, by OS/Platform.

4. Follow the configuration steps to configure the data collector. The instructions vary depending on the type of Operating System or Platform you are using to collect data.

 **HAProxy Configuration**
Gathers HAProxy metrics.

What Operating System or Platform Are You Using?

Ubuntu & Debian

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in your environment before configuring. [Show Instructions](#)

Follow Configuration Steps

Need Help?

- 1 Ensure that the HAProxy system you're going to gather metrics on has 'stats enable' option. For details refer to the following document.
- 2 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-haproxy.conf file.

```
# Read metrics of HAProxy, via socket or HTTP stats page
[[inputs.haproxy]]
  ## An array of address to gather stats about. Specify an ip or hostname
  ## with optional port, ie: localhost, 10.10.3.33:1938, etc.
  ## Make sure you specify the complete path to the stats endpoint
  ## <--> https://10.10.3.33:1938/haproxy?stats
```
- 3 Replace <INSERT_HAPROXY_ADDRESS> with the applicable HAProxy server address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT_HAPROXY_PORT> with the applicable HAProxy server port.
- 5 Modify the 'haproxy?stats' path in accordance to the HAProxy server configuration.
- 6 Modify 'username' and 'password' in accordance to the HAProxy server configuration (if credentials are required).
- 7 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 8 Restart the Telegraf service.

```
systemctl restart telegraf
```

Setup

Telegraf's plugin for HAProxy relies on HAProxy Stats enablement. This is a configuration built into HAProxy but it is not enabled out of the box. When enabled, HAProxy will expose an HTML endpoint that can be viewed on your browser or scraped for extraction of status of all HAProxy configurations.

Compatibility:

Configuration was developed against HAProxy version 1.9.4.

Setting Up:

To enable stats, edit your haproxy configuration file and add the the following lines after the 'defaults' section, using your own user/password and/or haproxy URL:

```
stats enable
stats auth myuser:mypassword
stats uri /haproxy?stats
```

The following is a simplified example configuration file with stats enabled:

```

global
  daemon
  maxconn 256

defaults
  mode http
  stats enable
  stats uri /haproxy?stats
  stats auth myuser:mypassword
  timeout connect 5000ms
  timeout client 50000ms
  timeout server 50000ms

frontend http-in
  bind *:80
  default_backend servers

frontend http-in9080
  bind *:9080
  default_backend servers_2

backend servers
  server server1 10.128.0.55:8080 check ssl verify none
  server server2 10.128.0.56:8080 check ssl verify none

backend servers_2
  server server3 10.128.0.57:8080 check ssl verify none
  server server4 10.128.0.58:8080 check ssl verify none

```

For complete and up to date instructions, see the [HAProxy documentation](#).

Objects and Counters

The following objects and their counters are collected:

Object:	Identifiers:	Attributes:	Datapoints:
HAProxy Frontend	Namespace Address Proxy	Node IP Node Name Proxy ID Mode Process id Sessions Rate Limit Server id Sessions Limit Status	Bytes In Bytes Out Cache Hits Cache Lookups Compression Bytes Bypassed Compression Bytes In Compression Bytes Out Compression Responses Connection Rate Connection Rate Max Connections Total Requests Denied by Connection Rule Requests Denied by Security Concerns Responses Denied by Security Concerns Requests Denied by Session Rule Requests Errors Responses 1xx Responses 2xx Responses 3xx Responses 4xx Responses 5xx Responses Other Requests Intercepted Sessions Rate Sessions Rate Max Requests Rate Requests Rate Max Requests Total Sessions Sessions Max Sessions Total Requests Rewrites

Object:	Identifiers:	Attributes:	Datapoints:
HAProxy Server	Namespace Address Proxy Server	Node IP Node Name Check Time to Finish Check Fall Configuration Check Health Value Check Rise Configuration Check Status Proxy ID Last Change Time Last Session Time Mode Process id Server id Status Weight	Active Servers Backup Servers Bytes In Bytes Out Check Downs Check Fails Client Aborts Connections Connection Average Time Downtime Total Denied Responses Connection Errors Response Errors Responses 1xx Responses 2xx Responses 3xx Responses 4xx Responses 5xx Responses Other Server Selected Total Queue Current Queue Max Queue Average Time Sessions per Second Sessions per Second Max Connection Reuse Response Time Average Sessions Sessions Max Server Transfer Aborts Sessions Total Sessions Total Time Average Requests Redispatches Requests Retries Requests Rewrites

Object:	Identifiers:	Attributes:	Datapoints:
HAProxy Backend	Namespace Address Proxy	Node IP Node Name Proxy ID Last Change Time Last Session Time Mode Process id Server id Sessions Limit Status Weight	Active Servers Backup Servers Bytes In Bytes Out Cache Hits Cache Lookups Check Downs Client Aborts Compression Bytes Bypassed Compression Bytes In Compression Bytes Out Compression Responses Connections Connection Average Time Downtime Total Requests Denied by Security Concerns Responses Denied by Security Concerns Connection Errors Response Errors Responses 1xx Responses 2xx Responses 3xx Responses 4xx Responses 5xx Responses Other Server Selected Total Queue Current Queue Max Queue Average Time Sessions per Second Sessions per Second Max Requests Total Connection Reuse Response Time Average Sessions Sessions Max Server Transfer Aborts Sessions Total Sessions Total Time Average Requests Redispatches Requests Retries Requests Rewrites

Troubleshooting

Additional information may be found from the [Support](#) page.

JVM Data Collector

Cloud Insights uses this data collector to gather metrics from JVM.

Installation

1. From **Admin > Data Collectors**, click **+Data Collector**. Under **Services**, choose JVM.

Select the Operating System or Platform on which the Telegraf agent is installed.

2. If you haven't already installed an Agent for collection, or you wish to install an Agent for a different Operating System or Platform, click *Show Instructions* to expand the **Agent installation** instructions.
3. Select the Agent Access Key for use with this data collector. You can add a new Agent Access Key by clicking the **+ Agent Access Key** button. Best practice: Use a different Agent Access Key only when you want to group data collectors, for example, by OS/Platform.
4. Follow the configuration steps to configure the data collector. The instructions vary depending on the type of Operating System or Platform you are using to collect data.



Java Configuration

Gathers JVM metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

RHEL & CentOS



Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)



[+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in your environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Install Jolokia on your JVMs. For details refer to the following document.
- 2 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-jvm.conf file.

```
# Read JMX metrics through Jolokia
[[inputs.jolokia2_agent]]
  # USER-ACTION: Provide address(es) of JVM, port for jolokia, add one URL for each JVM in
  # your cluster
  # Please specify actual machine IP address, and refrain from using a loopback address (i.e.
  # 127.0.0.1)
```



- 3 Replace <INSERT_JVM_ADDRESS> with the applicable JVM address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT_JOLOKIA_PORT> with the applicable JVM jolokia port.
- 5 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 6 Restart the Telegraf service.

```
systemctl restart telegraf
```



Setup

Information may be found in [JVM documentation](#).

Objects and Counters

The following objects and their counters are collected:

Object:	Identifiers:	Attributes:	Datapoints:
JVM	Namespace JVM	OS Architecture OS Name OS Version Runtime Specification Runtime Specification Vendor Runtime Specification Version Uptime Runtime VM Name Runtime VM Vendor Runtime VM Version Node Name Node IP	Class Loaded Class Loaded Total Class Unloaded Memory Heap Committed Memory Heap Init Memory Heap Used Max Memory Heap Used Memory Non Heap Committed Memory Non Heap Init Memory Non Heap Max Memory Non Heap Used Memory Objects Pending Finalization OS Processors Available OS Committed Virtual Memory Size OS Free Physical Memory Size OS Free Swap Space Size OS Max File Descriptor Count OS Open File Descriptors Count OS Processor CPU Load OS Processor CPU Time OS System CPU Load OS System Load Average OS Total Physical Memory Size OS Total Swap Space Size Thread Daemon Count Thread Peak Count Thread Count Thread Total Started Count Garbage Collector Copy Collection Count Garbage Collector Copy Collection Time Garbage Collector Mark- sweep Collection Count Garbage Collector Mark- sweep Collection Time Garbage Collector G1 Old Generation Collection Count Garbage Collector G1 Old Generation Collection Time Garbage Collector G1 Young Generation

Troubleshooting

Additional information may be found from the [Support](#) page.

Kafka Data Collector

Cloud Insights uses this data collector to gather metrics from Kafka.

Installation

1. From **Admin > Data Collectors**, click **+Data Collector**. Under **Services**, choose Kafka.
Select the Operating System or Platform on which the Telegraf agent is installed.
2. If you haven't already installed an Agent for collection, or you wish to install an Agent for a different Operating System or Platform, click *Show Instructions* to expand the [Agent installation](#) instructions.
3. Select the Agent Access Key for use with this data collector. You can add a new Agent Access Key by clicking the **+ Agent Access Key** button. Best practice: Use a different Agent Access Key only when you want to group data collectors, for example, by OS/Platform.
4. Follow the configuration steps to configure the data collector. The instructions vary depending on the type of Operating System or Platform you are using to collect data.



Kafka Configuration

Gathers Kafka metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows



Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)



+ Agent Access Key

*Please ensure that you have a Telegraf Agent in your environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Install Jolokia on your Kafka brokers. For details refer to the following document.
[Install Jolokia](#)
- 2 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-kafka.conf file.

```
# Read JMX metrics through Jolokia
[[inputs.jolokia2_agent]]
## USER-ACTION: Provide address(es) of kafka broker(s), port for jolokia, add one URL for
each broker in your cluster
## Please specify actual machine IP address, and refrain from using a loopback address (i.e.
#>127.0.0.1:8080
```

- 3 Replace <INSERT_KAFKA_BROKER_ADDRESS> with the applicable Kafka broker address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT_JOLOKIA_PORT> with the applicable Kafka broker jolokia port.
- 5 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 6 Modify 'Cluster' if needed for Kafka cluster designation.
- 7 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```



Setup

The Kafka plugin is based on the telegraf's Jolokia plugin. As such as a requirement to gather info from all Kafka brokers, JMX needs to be configured and exposed via Jolokia on all components.

Compatibility

Configuration was developed against Kafka version 0.11.0.2.

Setting up

All the instructions below assume your install location for kafka is '/opt/kafka'. You can adapt instructions below to reflect your install location.

Jolokia Agent Jar

A version the Jolokia agent jar file must be [downloaded](#). The version tested against was Jolokia agent 1.6.0.

Instructions below assume that the downloaded jar file (jolokia-jvm-1.6.0-agent.jar) is placed under the location '/opt/kafka/libs/'.

Kafka Brokers

To configure Kafka Brokers to expose the Jolokia API, you can add the following in <KAFKA_HOME>/bin/kafka-server-start.sh, just before the 'kafka-run-class.sh' call:

```
export JMX_PORT=9999
export RMI_HOSTNAME=`hostname -I`
export KAFKA_JMX_OPTS="-javaagent:/opt/kafka/libs/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0
-Dcom.sun.management.jmxremote.password.file=/opt/kafka/config/jmxremote.p
assword -Dcom.sun.management.jmxremote.ssl=false
-Djava.rmi.server.hostname=$RMI_HOSTNAME
-Dcom.sun.management.jmxremote.rmi.port=$JMX_PORT"
```

Note that example above is using 'hostname -I' to setup the 'RMI_HOSTNAME' environment variable. In multiple IP machines, this will need to be tweaked to gather the IP you care about for RMI connections.

You can choose a different port for JMX (9999 above) and Jolokia (8778). If you have an internal IP to lock Jolokia onto you can replace the "catch all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from the telegraf plugin. You can use the option '-Dcom.sun.management.jmxremote.authenticate=false' if you don't want to authenticate. Use at your own risk.

Objects and Counters

The following objects and their counters are collected:

Object:	Identifiers:	Attributes:	Datapoints:
Kafka Broker	Cluster Namespace Broker	Node Name Node IP	Replica Manager Fetcher Max Lag Zookeeper Client Connections Zookeeper Client Connections (15m rate) Zookeeper Client Connections (5m rate) Zookeeper Client Connections (mean rate) Zookeeper Client Connections (1m rate) Replica Manager Partition Count Thread Count Daemon Thread Count Peak Thread Count Current Thread Count Total Started Offline Partitions Produce Requests Total Time (50th Percentile) Produce Requests Total Time (75th Percentile) Produce Requests Total Time (95th Percentile) Produce Requests Total Time (98 Percentile) Produce Requests Total Time (999th Percentile) Produce Requests Total Time (99th Percentile) Produce Requests Total Time Produce Requests Total Time Max Produce Requests Total Time Mean Produce Requests Total Time Min Produce Requests Total Time Stddev Replica Manager ISR Shrinks Replica Manager ISR Shrinks (15m rate) Replica Manager ISR Shrinks (5m rate) Replica Manager ISR Shrinks (mean rate) Replica Manager ISR Shrinks (1m rate) Request Handler Avg Idle Request Handler Avg Idle

Troubleshooting

Additional information may be found from the [Support](#) page.

Kibana Data Collector

Cloud Insights uses this data collector to gather metrics from Kibana.

Installation

1. From **Admin > Data Collectors**, click **+Data Collector**. Under **Services**, choose Kibana.
Select the Operating System or Platform on which the Telegraf agent is installed.
2. If you haven't already installed an Agent for collection, or you wish to install an Agent for a different Operating System or Platform, click *Show Instructions* to expand the [Agent installation](#) instructions.
3. Select the Agent Access Key for use with this data collector. You can add a new Agent Access Key by clicking the **+ Agent Access Key** button. Best practice: Use a different Agent Access Key only when you want to group data collectors, for example, by OS/Platform.
4. Follow the configuration steps to configure the data collector. The instructions vary depending on the type of Operating System or Platform you are using to collect data.



Kibana Configuration

Gathers Kibana metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Ubuntu & Debian



Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)



[+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in your environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-kibana.conf file.

```
[[inputs.kibana]]  
## specify a list of one or more Kibana servers  
## USER-ACTION: Provide address of kibana server(s), port(s) for kibana server  
## Please specify actual machine IP address, and refrain from using a loopback address (i.e.  
localhost or 127.0.0.1).  
##
```



- 2 Replace <INSERT_KIBANA_ADDRESS> with the applicable Kibana server address. Please specify a real machine address, and refrain from using a loopback address.

- 3 Replace <INSERT_KIBANA_PORT> with the applicable Kibana server port.

- 4 Replace 'username' and 'pa\$\$word' with the applicable Kibana server authentication credentials as needed, and uncomment the lines.

- 5 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).

- 6 Restart the Telegraf service.

```
systemctl restart telegraf
```



Setup

Information may be found in the [Kibana documentation](#).

Objects and Counters

The following objects and their counters are collected:

Object:	Identifiers:	Attributes:	Datapoints:
Kibana	Namespace Address	Node IP Node Name Version Status	Concurrent Connections Heap Max Heap Used Requests per Second Response Time Average Response Time Max Uptime

Troubleshooting

Additional information may be found from the [Support](#) page.

Memcached Data Collector

Cloud Insights uses this data collector to gather metrics from Memcached.

Installation

1. From **Admin > Data Collectors**, click **+Data Collector**. Under **Services**, choose Memcached.
Select the Operating System or Platform on which the Telegraf agent is installed.
2. If you haven't already installed an Agent for collection, or you wish to install an Agent for a different Operating System or Platform, click *Show Instructions* to expand the [Agent installation](#) instructions.
3. Select the Agent Access Key for use with this data collector. You can add a new Agent Access Key by clicking the **+ Agent Access Key** button. Best practice: Use a different Agent Access Key only when you want to group data collectors, for example, by OS/Platform.
4. Follow the configuration steps to configure the data collector. The instructions vary depending on the type of Operating System or Platform you are using to collect data.



Memcached Configuration

Gathers Memcached metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows



Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)



[+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in your environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-memcached.conf file.

```
[[inputs.memcached]]  
## USER-ACTION: Provide comma-separated list of Memcached IP(s) and port(s).  
## Please specify actual machine IP address, and refrain from using a loopback address  
(i.e. localhost or 127.0.0.1).  
## When configuring with multiple Memcached servers, enter them in the format ["server1"  
" " " " ]
```



- 2 Replace <INSERT_MEMCACHED_ADDRESS> with the applicable Memcached server address. Please specify a real machine address, and refrain from using a loopback address.

- 3 Replace <INSERT_MEMCACHED_PORT> with the applicable Memcached server port.

- 4 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```



Setup

Information may be found in the [Memcached wiki](#).

Objects and Counters

The following objects and their counters are collected:

Object:	Identifiers:	Attributes:	Datapoints:
Memcached	Namespace Server	Node IP Node Name	Accepting Connections Handled Authentication Requests Failed Authentications Bytes Used Bytes Read (per sec) Bytes Written (per sec) CAS Badval CAS Hits CAS Misses Flush Reqs (per sec) Get Reqs (per sec) Set Reqs (per sec) Touch Reqs (per sec) Connection Yields (per sec) Connection Structures Open Connections Current Stored Items Decr Requests Hits (per sec) Decr Requests Misses (per sec) Delete Requests Hits (per sec) Delete Requests Misses (per sec) Items Evicted Valid Evictions Expired Items Get Hits (per sec) Get Misses (per sec) Used Hash Bytes Hash Is Expanding Hash Power Level Incr Requests Hits (per sec) Incr Requests Misses (per sec) Server Max Bytes Listen Disabled Num Reclaimed Worker Threads Count Total Opened Connections Total Items Stored Touch Hits Touch Misses Server Uptime

Troubleshooting

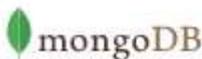
Additional information may be found from the [Support](#) page.

MongoDB Data Collector

Cloud Insights uses this data collector to gather metrics from MongoDB.

Installation

1. From **Admin > Data Collectors**, click **+Data Collector**. Under **Services**, choose MongoDB.
Select the Operating System or Platform on which the Telegraf agent is installed.
2. If you haven't already installed an Agent for collection, or you wish to install an Agent for a different Operating System or Platform, click *Show Instructions* to expand the [Agent installation](#) instructions.
3. Select the Agent Access Key for use with this data collector. You can add a new Agent Access Key by clicking the **+ Agent Access Key** button. Best practice: Use a different Agent Access Key only when you want to group data collectors, for example, by OS/Platform.
4. Follow the configuration steps to configure the data collector. The instructions vary depending on the type of Operating System or Platform you are using to collect data.



MongoDB Configuration

Gathers MongoDB metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

RHEL & CentOS

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

[+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in your environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Open mongod.conf. Locate the line beginning with "bindIp", and append the address of the node on which the Telegraf agent resides. After saving the change, restart the MongoDB server.
- 2 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-mongodb.conf file.

```
[[inputs.mongodb]]  
  ## An array of URLs of the form:  
  ## "mongodb://" [user ":" pass "@" host [ ":" port]  
  ## For example:  
  ##   mongodb://user:auth_key@10.10.3.38:27017,  
  ##   ...  
  ##   ...
```

- 3 Replace <INSERT_MONGODB_ADDRESS> with the applicable MongoDB server address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT_MONGODB_PORT> with the applicable MongoDB port.
- 5 Restart the Telegraf service.

```
systemctl restart telegraf
```

Setup

Information may be found in the [MongoDB documentation](#).

Objects and Counters

The following objects and their counters are collected:

Object:	Identifiers:	Attributes:	Datapoints:
MongoDB	Namespace Hostname		
MongoDB Database	Namespace Hostname Database name		

Troubleshooting

Information may be found from the [Support](#) page.

MySQL Data Collector

Cloud Insights uses this data collector to gather metrics from MySQL.

Installation

- From **Admin > Data Collectors**, click **+Data Collector**. Under **Services**, choose MySQL.
Select the Operating System or Platform on which the Telegraf agent is installed.
- If you haven't already installed an Agent for collection, or you wish to install an Agent for a different Operating System or Platform, click *Show Instructions* to expand the [Agent installation](#) instructions.
- Select the Agent Access Key for use with this data collector. You can add a new Agent Access Key by clicking the **+ Agent Access Key** button. Best practice: Use a different Agent Access Key only when you want to group data collectors, for example, by OS/Platform.
- Follow the configuration steps to configure the data collector. The instructions vary depending on the type of Operating System or Platform you are using to collect data.



MySQL Configuration

Gathers MySQL metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows



Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)



Agent Access Key

*Please ensure that you have a Telegraf Agent in your environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-mysql.conf file.

```
[[inputs.mysql]]  
## USER-ACTION: Provide comma-separated list of MySQL credentials, IP(s), and port(s)  
## e.g. servers = ["user:passwd@tcp(127.0.0.1:3306)/?tls=false"]  
## Please specify actual machine IP address, and refrain from using a loopback address  
(i.e. localhost or 127.0.0.1).  
##
```



- 2 Review and verify the contents of the configuration file.
- 3 Replace <INSERT_USERNAME> and <INSERT_PASSWORD> with the applicable MySQL credentials.
- 4 Replace <INSERT_PROTOCOL> with the applicable MySQL connection protocol. The typical protocol is tcp.
- 5 Replace <INSERT_MYSQL_ADDRESS> with the applicable MySQL server address. Please specify a real machine address, and refrain from using a loopback address.
- 6 Replace <INSERT_MYSQL_PORT> with the applicable MySQL server port. The typical port is 3306.
- 7 Modify the 'tls' parameter in accordance to the MySQL server configuration.
- 8 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```



Setup

Information may be found in the [MySQL documentation](#).

Objects and Counters

The following objects and their counters are collected:

Object:	Identifiers:	Attributes:	Datapoints:
MySQL	Namespace MySQL Server	Node IP Node Name	Aborted Clients (per sec) Aborted Connects (per sec) RX Bytes (per sec) TX Bytes (per sec) Commands Admin (per sec) Commands Alter Event Commands Alter Function Commands Alter Instance Commands Alter Procedure Commands Alter Server Commands Alter Table Commands Alter Tablespace Commands Alter User Commands Analyze Commands Assign To Keycache Commands Begin Commands Binlog Commands Call Procedure Commands Change DB Commands Change Master Commands Change Repl Filter Commands Check Commands Checksum Commands Commit Commands Create DB Commands Create Event Commands Create Function Commands Create Index Commands Create Procedure Commands Create Server Commands Create Table Commands Create Trigger Commands Create UDF Commands Create User Commands Create View Commands Dealloc SQL Connection Errors Accept Created Tmp Disk Tables Delayed Errors Flush Commands Handler Commit Innodb Buffer Pool Bytes Data Key Blocks Not Flushed

Troubleshooting

Additional information may be found from the [Support](#) page.

Netstat Data Collector

Cloud Insights uses this data collector to gather Netstat metrics.

Installation

1. From **Admin > Data Collectors**, click **+Data Collector**. Under **Services**, choose Netstat.
Select the Operating System or Platform on which the Telegraf agent is installed.
2. If you haven't already installed an Agent for collection, or you wish to install an Agent for a different Operating System or Platform, click *Show Instructions* to expand the [Agent installation](#) instructions.
3. Select the Agent Access Key for use with this data collector. You can add a new Agent Access Key by clicking the **+ Agent Access Key** button. Best practice: Use a different Agent Access Key only when you want to group data collectors, for example, by OS/Platform.
4. Follow the configuration steps to configure the data collector. The instructions vary depending on the type of Operating System or Platform you are using to collect data.

netstat

Netstat Configuration

Gathers netstat metrics of the host where telegraf agent is installed.

What Operating System or Platform Are You Using?

[Need Help?](#)



Windows



Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)



[+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in your environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-netstat.conf file.

```
# Read TCP metrics such as established, time wait and sockets counts.  
[[inputs.netstat]]  
# no configuration  
[inputs.netstat.tags]  
CloudInsights = "true"
```



- 2 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```



Setup

Objects and Counters

The following objects and their counters are collected:

Object:	Identifiers:	Attributes:	Datapoints:
Netstat	Node UUID	Node IP Node Name	

Troubleshooting

Additional information may be found from the [Support](#) page.

Nginx Data Collector

Cloud Insights uses this data collector to gather metrics from Nginx.

Installation

1. From Admin > Data Collectors, click **+Data Collector**. Under **Services**, choose Nginx.

Select the Operating System or Platform on which the Telegraf agent is installed.

2. If you haven't already installed an Agent for collection, or you wish to install an Agent for a different Operating System or Platform, click *Show Instructions* to expand the [Agent installation](#) instructions.
3. Select the Agent Access Key for use with this data collector. You can add a new Agent Access Key by clicking the **+ Agent Access Key** button. Best practice: Use a different Agent Access Key only when you want to group data collectors, for example, by OS/Platform.
4. Follow the configuration steps to configure the data collector. The instructions vary depending on the type of Operating System or Platform you are using to collect data.

The screenshot shows the 'Nginx Configuration' page. At the top, there's a logo for NGINX and a brief description: 'Gathers Nginx metrics.' Below this, a section titled 'What Operating System or Platform Are You Using?' contains a dropdown menu set to 'Ubuntu & Debian'. To the right of the dropdown is a 'Need Help?' link. A large blue button labeled '+ Agent Access Key' is positioned below the dropdown. At the bottom of the page, a note reads: '*Please ensure that you have a Telegraf Agent in your environment before configuring. [Show Instructions](#)'.

Follow Configuration Steps

Need Help?

- 1 If you already have a URL enabled to provide Nginx metrics, go directly to the plugin configuration.
- 2 Nginx metrics are available through a status page when the HTTP stub status module is enabled. Refer to the below link for verifying/enabling `http_stub_status_module`.
http://nginx.org/en/docs/http/ngx_http_stub_status_module.html

- 3 After verifying the module is enabled, modify the Nginx configuration to set up a locally-accessible URL for the status page:

```
server {  
    listen <PORT NUMBER>;  
    Please specify actual machine IP address, and refrain from using a loopback address (i.e.  
localhost or 127.0.0.1)  
    server_name <IP ADDRESS>;  
    location /nginx_status {  
        ...  
    }  
}
```

- 4 Reload the configuration:

```
nginx -s reload
```

- 5 Copy the contents below into a new .conf file under the `/etc/telegraf/telegraf.d` directory. For example, copy the contents to the `/etc/telegraf/telegraf.d/cloudinsights-nginx.conf` file.

```
[[inputs.nginx]]  
## USER-ACTION: Provide Nginx status url.  
## Please specify actual machine IP address where nginx_status is enabled, and refrain from  
## using a loopback address (i.e. localhost or 127.0.0.1).  
## When configuring with multiple Nginx servers, enter them in the format ["url1", "url2",  
## ...]
```

- 6 Replace `<INSERT_NGINX_ADDRESS>` with the applicable Nginx address. Please specify a real machine address, and refrain from using a loopback address.

- 7 Replace `<INSERT_NGINX_PORT>` with the applicable Nginx port.

- 8 Restart the Telegraf service.

```
systemctl restart telegraf
```

Setup

Nginx metric collection requires that Nginx `http_stub_status_module` be enabled.

Additional information may be found in the [Nginx documentation](#).

Objects and Counters

The following objects and their counters are collected:

Object:	Identifiers:	Attributes:	Datapoints:
Nginx	Namespace Server	Node IP Node Name Port	Accepts Active Handled Reading Requests Waiting Writing

Troubleshooting

Additional information may be found from the [Support](#) page.

PostgreSQL Data Collector

Cloud Insights uses this data collector to gather metrics from PostgreSQL.

Installation

1. From **Admin > Data Collectors**, click **+Data Collector**. Under **Services**, choose PostgreSQL.
Select the Operating System or Platform on which the Telegraf agent is installed.
2. If you haven't already installed an Agent for collection, or you wish to install an Agent for a different Operating System or Platform, click *Show Instructions* to expand the [Agent installation](#) instructions.
3. Select the Agent Access Key for use with this data collector. You can add a new Agent Access Key by clicking the **+ Agent Access Key** button. Best practice: Use a different Agent Access Key only when you want to group data collectors, for example, by OS/Platform.
4. Follow the configuration steps to configure the data collector. The instructions vary depending on the type of Operating System or Platform you are using to collect data.



PostgreSQL

PostgreSQL Configuration

Gathers PostgreSQL metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

RHEL & CentOS



Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

[+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in your environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-postgresql.conf file.

```
[[inputs.postgresql]]  
# USER-ACTION: Provide credentials for access, address of PostgreSQL server, port for  
PostgreSQL server, one DB for access  
address = "postgres://<INSERT_USERNAME>:<INSERT_PASSWORD>@<INSERT_POSTGRESQL_ADDRESS>:  
<INSERT_POSTGRESQL_PORT>/<INSERT_DB>"
```

- 2 Replace <INSERT_USERNAME> and <INSERT_PASSWORD> with the applicable PostgreSQL credentials.

- 3 Replace <INSERT_POSTGRESQL_ADDRESS> with the applicable PostgreSQL address. Please specify a real machine address, and refrain from using a loopback address.

- 4 Replace <INSERT_POSTGRESQL_PORT> with the applicable PostgreSQL port.

- 5 Replace <INSERT_DB> with the applicable PostgreSQL database.

- 6 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).

- 7 Restart the Telegraf service.

```
systemctl restart telegraf
```



Setup

Information may be found in the [PostgreSQL documentation](#).

Objects and Counters

The following objects and their counters are collected:

Object:	Identifiers:	Attributes:	Datapoints:
PostgreSQL Server	Namespace Database Server	Node Name Node IP	Buffers Allocated Buffers Backend Buffers Backend File Sync Buffers Checkpoint Buffers Clean Checkpoints Sync Time Checkpoints Write Time Checkpoints Requests Checkpoints Timed Max Written Clean
PostgreSQL Database	Namespace Database Server	Database OID Node Name Node IP	Blocks Read Time Blocks Write Time Blocks Hits Blocks Reads Conflicts Deadlocks Client Number Temp Files Bytes Temp Files Number Rows Deleted Rows Fetched Rows Inserted Rows Returned Rows Updated Transactions Committed Transactions Rollbacked

Troubleshooting

Additional information may be found from the [Support](#) page.

Puppet Agent Data Collector

Cloud Insights uses this data collector to gather metrics from Puppet Agent.

Installation

- From **Admin > Data Collectors**, click **+Data Collector**. Under **Services**, choose Puppet.
Select the Operating System or Platform on which the Telegraf agent is installed.
- If you haven't already installed an Agent for collection, or you wish to install an Agent for a different Operating System or Platform, click *Show Instructions* to expand the **Agent installation** instructions.
- Select the Agent Access Key for use with this data collector. You can add a new Agent Access Key by clicking the **+ Agent Access Key** button. Best practice: Use a different Agent Access Key only when you want to group data collectors, for example, by OS/Platform.
- Follow the configuration steps to configure the data collector. The instructions vary depending on the type of Operating System or Platform you are using to collect data.



Puppet Agent Configuration

Gathers Puppet agent metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

[+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in your environment before configuring [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-puppetagent.conf file.

```
## Reads last_run_summary.yaml file and converts to measurements
[[inputs.puppetagent]]
  ## Location of puppet last run summary file
  ## USER-ACTION: Modify the location if last_run_summary.yaml is on different path
  location = "/var/lib/puppet/state/last_run_summary.yaml"
```

- 2 Modify 'location' if last_run_summary.yaml is on different path

- 3 Modify 'Namespace' if needed for puppet agent disambiguation (to avoid name clashes).

- 4 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```



Setup

Information may be found in the [Puppet documentation](#)

Objects and Counters

The following objects and their counters are collected:

Object:	Identifiers:	Attributes:	Datapoints:

Puppet Agent	Namespace Node UUID	Node Name Location Node IP Version Configstring Version Puppet	Changes Total Events Failure Events Success Events Total Resources Changed Resources Failed Resources Failed To Restart Resources Outofsync Resources Restarted Resources Scheduled Resources Skipped Resources Total Time Anchor Time Configretrieval Time Cron Time Exec Time File Time Filebucket Time Lastrun Time Package Time Schedule Time Service Time Sshauthorizedkey Time Total Time User
--------------	------------------------	--	--

Troubleshooting

Additional information may be found from the [Support](#) page.

Redis Data Collector

Cloud Insights uses this data collector to gather metrics from Redis. Redis is an open source, in-memory data structure store used as a database, cache, and message broker, supporting the following data structures: strings, hashes, lists, sets, and more.

Installation

- From **Admin > Data Collectors**, click **+Data Collector**. Under **Services**, choose Redis.
Select the Operating System or Platform on which the Telegraf agent is installed.
- If you haven't already installed an Agent for collection, or you wish to install an Agent for a different Operating System or Platform, click *Show Instructions* to expand the [Agent installation](#) instructions.
- Select the Agent Access Key for use with this data collector. You can add a new Agent Access Key by clicking the **+ Agent Access Key** button. Best practice: Use a different Agent Access Key only when you want to group data collectors, for example, by OS/Platform.
- Follow the configuration steps to configure the data collector. The instructions vary depending on the type of Operating System or Platform you are using to collect data.



Redis Configuration

Gathers Redis metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows



Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)



Agent Access Key

*Please ensure that you have a Telegraf Agent in your environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- Configure Redis to accept connections from the address of the node on which the Telegraf agent resides. Open the Redis configuration file.

```
vi /etc/redis.conf
```



- Locate the line that begins with 'bind 127.0.0.1', and append the address of the node on which the Telegraf agent resides

```
bind 127.0.0.1 <NODE_IP_ADDRESS>
```



- Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-redis.conf file.

```
# Read metrics from one or many redis servers
[[inputs.redis]]
  ## specify servers via a url matching:
  ## [protocol://[:password]@address[:port]
  ## e.g.
  ## -----
```



- Replace <INSERT_REDIS_ADDRESS> with the applicable Redis address. Please specify a real machine address, and refrain from using a loopback address.

- Replace <INSERT_REDIS_PORT> with the applicable Redis port.

- Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```



Setup

Information may be found in the [Redis documentation](#).

Objects and Counters

The following objects and their counters are collected:

Object:	Identifiers:	Attributes:	Datapoints:
Redis	Namespace Server		

Troubleshooting

Additional information may be found from the [Support](#) page.

Object Icon Reference

A quick reference for object icons used in Cloud Insights.

Storage	Networking	Compute	Application	Misc.
Backend Storage Array	Fabric	Datastore		Unknown
Backend Volume	iSCSI Network Portal	Host		Generic
Disk	iSCSI Session	Virtual Machine		Violation
Internal Volume	NAS	VMDK		Failure
Masking	NPV Switch			
Path	NPV Chassis			
Q-Tree	Port			
Quota	Switch			
Share	Zone			
Storage	Zone Members			
Storage Node				
Storage Pool				
Tape				
Volume				
Virtual Storage Array				
Virtual Volume				

Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

<http://www.netapp.com/us/legal/copyright.aspx>

Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

Patents

A current list of NetApp owned patents can be found at:

<https://www.netapp.com/us/media/patents-page.pdf>

Privacy policy

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

[Notice for Cloud Insights](#)

[Notice for Workload Security \(formerly Cloud Secure\)](#)

Copyright information

Copyright © 2023 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—with prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.