NetApp

Cloud Insights

NetApp
September 08, 2022

Table of Contents

NetApp

NetApp Astra Data Store data collector

This data collector acquires inventory and performance data for a single Astra Data Store cluster. In addition to the data collector, the Monitoring Operator will collect advanced metrics as well as configure *Fluent Bit* to collect logs.

> These installation instructions and additional information can also be found in the Astra Data Store documentation:
> Monitor metrics with Cloud Insights
> Quick start for Astra Data Store

Terminology

Cloud Insights acquires inventory and performance data 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
AstraDSVolume	Internal Volume
AstraDSNodeInfo.status.drives	Disk
AstraDSNodeInfo	Storage Node
AstraDSExportPolicy	Share / Share Initiator
AstraDSCluster	Storage

Requirements

- The NetApp Monitoring Operator must be installed in the Kubernetes cluster with Astra Data Store. If this was not installed during the Astra Data Store installation, please install the monitoring operator following the Astra Data Store installation instructions.

- The *kubectl-astrads* kubectl plugin must be installed. If it is not installed, please install the *kubectl-astrads* binary following the Astra Data Store installation instructions.

- The following commands must be available: *awk, curl, grep and jq*.

Installation

The installation script will walk you through installation of the Astra Data Store data collector. Follow the instructions on-screen. Installation will take several minutes to complete. Once complete, it may take a few more minutes before data is shown in Cloud Insights.

The script will walk you through the following steps:

1. Choose an API Access Token.

2. Copy the installer script from the installation dialog and save it as as a file named *cloudinsights-ads-monitoring.sh*. You can click the clipboard icon to quickly copy the script to the clipboard.

3. Open a Bash window, change directory to the location of the *cloudinsights-ads-monitoring.sh* script.

4. Copy the permissions command block from the installation dialog. You can click the clipboard icon to quickly copy the command to the clipboard.

5. Paste the permissions command into the Bash window and press Enter.

6. Copy the install command from the installation dialog. You can click the clipboard icon to quickly copy the command to the clipboard.

7. Paste the install command into the Bash window.

8. Replace <KUBERNETES_IP> with the IP address of the Kubernetes API server.

9. Replace <KUBERNETES_TOKEN> with your Kubernetes API token.

10. Press Enter.

    The installer script will:
    * Verify the Monitoring Operator is installed and configured.
    * Configure Fluent Bit.
    * Install the Acquisition Unit.
    * Install the Astra Data Store collector once the Acquisition Unit is running.

11. Click *Complete Setup*.

If the installer script exits due to an error, you can rerun it again once the error is resolved. The installer script supports additional parameters such as the Monitoring Operator namespace and Kubernetes API server port if your environment does not use the default settings. A full list of available options is listed below.

Installer script options:

Note that the Cloud Insights domain name and selected API Access Key will be embedded in the installer script when it is downloaded.

```
$ ./cloudinsights-ads-monitoring.sh -h
USAGE: cloudinsights-ads-monitoring.sh [OPTIONS]
Configure monitoring of Astra Data Store by Cloud Insights.
OPTIONS:
 -h                      Display this help message.
 -d ci_domain_name       Cloud Insights tenant domain name.
 -i kubernetes_ip        Kubernetes API server IP address.
 -k ci_api_key           Cloud Insights API Access Key.
 -n namespace            Namespace for monitoring components. (default:
netapp-monitoring)
 -p kubernetes_port      Kubernetes API server port. (default: 6443)
 -r root_pv_dir          Create 3 Persistent Volumes in this directory for
the Acquisition Unit.
                         Only specify this option if there is no Storage
Provisioner installed and the PVs do not already exist.
 -s storage_class        Storage Class name for provisioning Acquisition
Unit PVs. If not specified, the default storage class will be used.
 -t kubernetes_token     Kubernetes API server token.
```

Troubleshooting

Some things to try if you encounter problems with this data collector:

Astra Data Store data collector

Problem:	Try this:
You see an "Unauthorized" message	Check that the Kubernetes API Token has permission to call APIs in the *astrads.netapp.io* apiGroup
"Unknown host: astrads-metrics-service.astrads-system.svc.cluster.local: Name or service not known"	Verify the collector is installed in an Acquisition Unit pod running inside the ADS Kubernetes cluster. Verify the astrads-metrics-service is running the astrads-system namespace.

Installation Script

Problem:	Try this:
The monitoring operator is not running in <namespace> namespace.	Follow the Astra Data Store installation instructions to install it
Acquisition Unit pod <pod> did not start successfully after 300 seconds.	Get the name of the acquisition unit pod: kubectl get pods --namespace netapp-monitoring | grep "au-pod" Check the pod events for errors: kubectl describe pod --namespace netapp-monitoring <POD_NAME>
Acquisition Unit installation has not finished after 900 seconds	Get the name of the acquisition unit pod: kubectl get pods --namespace netapp-monitoring | grep "au-pod" Check the pod logs for errors: kubectl logs --namespace netapp-monitoring <POD_NAME> If there are no errors and the logs end with the message "Main - Acquisition is up and running!", the install succeeded but too longer than expected. Rerun the installation script.
Failed to retrieve Acquisition Unit id from Cloud Insights	Verify the Acquisition Unit appears in Cloud Insights. Go to Admin > Data Collectors and click on the Acquisition Units tab. Verify the Cloud Insights API key has permission for Acquisition Unit.

Additional information on this Data Collector may be found from the Support page or in the Data Collector Support Matrix.

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.

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.

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.

- 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.
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.

Field	Description
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

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.

> ⓘ Config Advisor is considered a *Preview* feature and is therefore subject to change. During Preview, no MU cost is incurred.

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
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:

[] | *Installing and Configuring the Config Advisor data collector*

Creating a Config Advisor dashboard:

[] | *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 *file* or *shell*. The default is *shell*.
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.
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 SSLException	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: > *system node systemshell -node * -command "spmctl -h cmd –stop; spmctl -h cmd –exec"*

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:

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	Check whether the user has the following permission on the device: • api-* • cli-date • cli-df • cli-ifconfig • cli-lun • cli-operations • cli-rdfile • cli-snap • login-http-admin • security-api-vfiler Also check if the ONTAP version is supported by Cloud Insights and verify if the credentials used match device credentials
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

Problem:	Try this:
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 SSLException	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.
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 value 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

Vendor/Model Term	Cloud Insights Term
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)	Deafult 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	Possible solutions: * 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	Possible solutions: * 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.