



Reference & Support

Cloud Insights

NetApp
September 22, 2022

This PDF was generated from https://docs.netapp.com/us-en/cloudinsights/concept_requesting_support.html on September 22, 2022. Always check docs.netapp.com for the latest.

Table of Contents

- Reference & Support 1
 - Requesting Support 1
 - Cloud Insights Data Collector Support Matrix 6
 - Data Collector Reference - Infrastructure 6
 - Data Collector Reference - Services 109
 - Object Icon Reference 190

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.

| | | | |
|---|--|--|--|
| Cloud Insights Support NetApp Serial Number: 123456789011234567890 AWS Customer ID: AbCdEfGhI1234567890zyxWVU Support activation is required to enable support with NetApp through web ticket or phone. Activate Support at register.netapp.com . <input checked="" type="checkbox"/> Check this box to allow NetApp access to your instance of Cloud Insights. | Contact Us Need help with Cloud Insights? Technical Support: Open a Support Ticket Phone (P1) Chat Sales: Have questions regarding your subscription? Contact Sales . | | |
| Knowledge Base Search through the Cloud Insights Knowledge Base to find helpful articles. | Documentation Center Visit the Cloud Insights Documentation Center to find step by step instructions to help you get the most out of Cloud Insights. | Communities Join the Cloud Insights Community to follow ongoing discussions or create a new one. | Feedback We value your input. Your feedback helps us improve Cloud Insights. |
| Learning Center Cloud Insights Course List: <ul style="list-style-type: none">• Hybrid Cloud Resource Management• Cloud Insights Fundamentals• Cloud Resource Management• Cloud Secure Cloud Education All-Access Pass: Visit and subscribe the Cloud Education All-Access Pass to get unlimited access to our best cloud learning resources. Course Catalog: Browse the Learning Services Product Catalog to find all the courses that are relevant to you. | | | |
| Proxy Settings Need to setup proxy exceptions? Click here to learn more. | | | |



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: | NetApp Subscription Name: |
| 95011122233344455512 | 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 # * ⓘ | <input type="text" value="e.g. 95012235021303893918"/> |
| NetApp Subscription Name * ⓘ | <input type="text" value="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"/> |
| State/Province / Country* | <input type="text"/> - Select - <input type="button" value="v"/> |
| 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* | Cloud Insights <input type="button" value="v"/> |
| Billing Provider * | NetApp <input type="button" value="v"/> |
| Cloud Insights Serial # * <input type="button" value="i"/> | <input type="text" value="e.g. 95012235021303893918"/> |
| NetApp Subscription Name * <input type="button" value="i"/> | <input type="text" value="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:
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.

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.

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):

City (optional): State/Province (optional):

Postal Code (optional): Country (optional): **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. |
| 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](#)

[Creating a Role to Delegate Permissions to an IAM User](#)

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 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".
- 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.

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 |

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 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. |

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) |
| 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 |

| Vendor/Model Term | Cloud Insights Term |
|-------------------|---------------------|
| 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 |

| Field | Description |
|--------------------------------------|---|
| 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. |
| 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: <date> <time> ERROR [com.onaro.sanscreen.acquisition.framework.datasource.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) | 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) |
| 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 Alais 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. |

| Field | Description |
|---------------------------------|--|
| 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 |
| 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 |

| Field | Description |
|---------------|---|
| 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" | <ul style="list-style-type: none"> * Verify that the user has permissions to run the following commands on the device: <ul style="list-style-type: none"> > 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. |
| 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. |

| Field | Description |
|--------------------------|--------------------|
| 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 |
| 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 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\SYMAPI\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 sstorage 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.

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>netcnfg</i> file |

| Field | Description |
|-----------------------|--|
| 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 |
| Connection Caching | <p>Choose connection caching method:</p> <p>* 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.</p> <p>* 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.</p> <p>* 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> <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 |

| Field | Description |
|--|---|
| Performance Polling Interval (sec) | Interval between performance polls (default 1000 seconds) |
| hoose '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:

Inventory

| 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 |

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. |

| Field | Description |
|----------------------------|---|
| 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: <ul style="list-style-type: none"> • 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 |

| Problem: | Try this: |
|--|--|
| 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" |
| 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 |

| Vendor/Model Term | Cloud Insights Term |
|-------------------------------------|---------------------|
| 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 accordingly • Wait 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 correctly • Please 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 XtremIO (HTTP) data collector, you must have:

- The XtremIO 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 XtremIO 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 XtremIO Management Server (XMS) Host IP address
- Administrator user name and password for the XtremIO

Configuration

| Field | Description |
|-----------|--|
| XMS Host | IP address or fully-qualified domain name of the XtremIO Management Server |
| User name | User name for the XtremIO Management Server |
| Password | Password for the XtremIO Management Server |

Advanced configuration

| Field | Description |
|---------------------------------|--|
| TCP port | TCP Port used to connect to XTremIO Management Server. The default is 443. |
| 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](#).

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 |

| Vendor/Model Term | Cloud Insights Term |
|---|---------------------|
| 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" | <p>Likely caused by: Storage system has page scrolling enabled.</p> <p>Possible solution:</p> <p>* Try to disable page scrolling by running the following command:</p> <p>set clienv-show-more -scroll disable</p> |

| Problem: | Try this: |
|--|--|
| "Connecting error" with error messages "Failed to instantiate an SSH connection to storage" or "Failed to instantiate a connection to VirtualCenter" | Likely causes: <ul style="list-style-type: none"> * Incorrect credentials. * Incorrect IP address. * Network problem. * Storage may be down or unresponsive. Possible solutions: <ul style="list-style-type: none"> * 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. |

| Field | Description |
|--|---|
| 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 |

| Problem: | Try this: |
|--|--|
| Cloud Insights states that it cannot connect/login to SMI-S service. | <p>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.</p> <p>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.</p> <p>Verify that:</p> <ul style="list-style-type: none"> * Service is enabled * HTTPS is enabled * HTTPS port should be 5989 <p>If those all are so, you can try to “stopcim” and then a “startcim” to restart the CIM (i.e. SMI-S service).</p> |

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 "cisis" 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 |
| 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 | <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 |
| SNM2Devices - WMS/SMS/AMS Storages | <p>Device list for WMS/SMS/AMS storages. Each storage requires:</p> <ul style="list-style-type: none"> * 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 |

| Field | Description |
|---------------------------------------|---|
| 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. |
| 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 contains 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. |

| Problem: | Try this: |
|--|---|
| 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 |

| Vendor/Model Term | Cloud Insights Term |
|-------------------------|---------------------|
| 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 | 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 |

| Field | Description |
|------------------------------|--|
| 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 | * 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. |
| 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 contains 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. |

| Problem: | Try this: |
|--|---|
| 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 |

| Vendor/Model Term | Cloud Insights Term |
|-------------------|---------------------|
| 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 |

| Problem: | Try this: |
|---|--|
| "Error connecting " or "Invalid login credentials" with error messages "Could not communicate with the device:" | <ul style="list-style-type: none"> * 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 of the Ops Center server
- Read-only user name and password for the Ops Center software and peer privileges

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 ID's or array names 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 |

| Vendor/Model Term | Cloud Insights Term |
|----------------------|----------------------|
| 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. |
| 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 |
| 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 |
| 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 |

| Field | Description |
|---------------------------------|--|
| 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. |
| Error: * Cannot run program * Error executing command | <ul style="list-style-type: none"> * 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 |

| Vendor/Model Term | Cloud Insights Term |
|-------------------|---------------------|
| 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 |

| Field | Description |
|-------------------|--|
| 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. |

| 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](#).

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 |
| 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 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 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 <i>astrads.netapp.io</i> 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: <code>kubectl get pods --namespace netapp-monitoring grep "au-pod"</code> Check the pod events for errors: <code>kubectl describe pod --namespace netapp-monitoring <POD_NAME></code> |
| Acquisition Unit installation has not finished after 900 seconds | Get the name of the acquisition unit pod: <code>kubectl get pods --namespace netapp-monitoring grep "au-pod"</code> Check the pod logs for errors: <code>kubectl logs --namespace netapp-monitoring <POD_NAME></code> 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.

Connect to ONTAP 9.9+ via a Cloud Connection

[Need Help?](#)

- 1 
- 2 
- 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.



- 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 Volumes 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. |
| 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](#)

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 |

| 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:

[▶](#) | *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 <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 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. |
| <p>Additional Connection errors:</p> <p>ZAPI response has error code 13001, "database is not open"</p> <p>ZAPI error code is 60 and response contains "API did not finish on time"</p> <p>ZAPI response contains "initialize_session() returned NULL environment"</p> <p>ZAPI error code is 14007 and response contains "Node is not healthy"</p> | 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 | <p>This is usually due to perf stat not running. Try the following command on each node:</p> <pre>> system node systemshell -node * -command "spmctl -h cmd --stop; spmctl -h cmd --exec"</pre> |

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 |

| Vendor/Model Term | Cloud Insights Term |
|-------------------|---------------------|
| 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 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. |

| Problem: | Try this: |
|---|---|
| <p>Additional Connection errors:</p> <p>ZAPI response has error code 13001, "database is not open"</p> <p>ZAPI error code is 60 and response contains "API did not finish on time"</p> <p>ZAPI response contains "initialize_session() returned NULL environment"</p> <p>ZAPI error code is 14007 and response contains "Node is not healthy"</p> | <p>Check network, port number, and IP address. User should also try to run a command from command line from the AU machine.</p> |
| 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 | <p>Check that the acquiring user capabilities include the following at a minimum:</p> <ul style="list-style-type: none"> api-* security-api-vfiler login-http-admin <p>Confirm that filer is running minimum ONTAPI version 1.7.</p> |

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 throughput 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 |

| Problem: | Try this: |
|--|---|
| 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](#).

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. |

| 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](#).

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" | <p>Likely due to certain roles (for example, 'advanced_analytics') are not included for the configured user <userName>.</p> <p>Possible Solution:</p> <ul style="list-style-type: none">* 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 |
| 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](#).

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 |

| Field | Description |
|-----------|---|
| 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 |

| Problem: | Try this: |
|--|--|
| 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 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 | 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](#).

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 |

| Object: | Identifiers: | Attributes: | Datapoints: |
|-----------|-------------------|---------------------------------|--|
| 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:

```
Memory Used Total = Memory Total - 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:

```
Memory Used = App Memory + Wired Memory + 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 you 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.

- 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

[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 you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 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](#).
- 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.
  ## Please provide actual machine IP address and replace the value of localhost address if -
```
- Replace <INSERT_APACHE_ADDRESS> with the applicable Apache server address. Please specify a real machine address, and refrain from using a loopback address.
- Replace <INSERT_APACHE_PORT> with the applicable Apache server port.
- Modify the '/server-status' path in accordance to the Apache server configuration.
- 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

1. 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 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 you 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.
  ## http://username:password@127.0.0.1:8090
```

- 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

1. From **Admin > Data Collectors**, click **+Data Collector**. Under **Services**, choose CouchDB.

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.



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 you 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).
```

- 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

1. 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.



Docker Configuration
Gathers Docker 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 you 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-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 you 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_ELASTICSEARCH_ADDRESS> with the applicable Elasticsearch address. Please specify a real machine address, and refrain from using a loopback address.
- 3 Replace <INSERT_ELASTICSEARCH_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 Proccessors 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 you 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](#).
- 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  
  ## for each Job Manager to monitor metrics
```

- 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.



Hadoop Configuration

Gathers Hadoop metrics.

What Operating System or Platform Are You Using?

Ubuntu & Debian

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 you environment before configuring [Show Instructions](#)

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  
  ## Please provide explicit address(es) and provide each address a Jolokia address
```

- 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.p
assword"
```

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 Initing 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 Oppportunistic 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 Decomissioned Number NodeManager Decomissioning 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

1. From **Admin > Data Collectors**, click **+Data Collector**. Under **Services**, choose HAProxy.

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.



HAProxy Configuration

Gathers HAProxy 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 you 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 on hostname
  ## with optional port. ie localhost, 10.10.3.33:1936, etc.
  ## Make sure you specify the complete path to the stats endpoint
  ## including the context. ie http://10.10.3.33:1936/stats;jsessionid=...
```

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 you 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.
  # 192.168.1.1 or 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 you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Install Jolokia on your Kafka brokers. For details refer to the following [document](#).
- 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)
```

- 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 you 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 'password' 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 you 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 you 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@10.10.3.30:27017,
  ## mongodb://10.10.3.30:27017
```

- 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

1. From **Admin > Data Collectors**, click **+Data Collector**. Under **Services**, choose MySQL.

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.



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 you 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 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 you environment before configuring [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 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"
```
- 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.



Nginx Configuration
Gathers Nginx 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 you 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/nginx_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 {  
        stub_status on;  
    }  
}
```

- 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",  
  "url3"]
```

- 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 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 you 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 Rolledback |

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

1. From **Admin > Data Collectors**, click **+Data Collector**. Under **Services**, choose Puppet.

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.



Puppet Agent Configuration

Gathers Puppet agent 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 you 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

1. From **Admin > Data Collectors**, click **+Data Collector**. Under **Services**, choose Redis.

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.



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 you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 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
```



- 2 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>
```



- 3 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.
  ## tcp://username@192.168.0.1:6379
```



- 4 Replace <INSERT_REDIS_ADDRESS> with the applicable Redis address. Please specify a real machine address, and refrain from using a loopback address.
- 5 Replace <INSERT_REDIS_PORT> with the applicable Redis port.
- 6 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 |  Application |  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 | | | | |

Copyright Information

Copyright © 2022 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-without 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.