Splunk® Supported Add-ons
Splunk Add-on for NetApp Data ONTAP released

Generated: 11/01/2022 6:16 am

Table of Contents

Overview

About the Splunk Add-on for NetApp Data ONTAP

Version	3.0.3
Vendor Products	NetApp Data ONTAP
Visible in Splunk Web	Yes. This add-on contains views for configuration.

The Splunk Add-on for NetApp Data ONTAP makes API calls directly to your NetApp filers to collect API data and forwards that data to your Splunk deployment, and allows a Splunk software administrator to collect data related to:

- Performance
- Inventory
- Options
- EMS data

The Splunk Add-on for NetApp Data ONTAP works with versions 2.1.91 or later of the Splunk App for NetApp Data ONTAP and versions 2.6.0 and later of the Storage Module for IT Service Intelligence.

This add-on provides modular inputs and CIM-compatible knowledge to use with other Splunk products, such as Splunk IT Service Intelligence and the Splunk App NetApp Data ONTAP.

The Splunk Add-on for NetApp Data ONTAP contains the following components:

- Splunk_TA_ontap 3.0.3
- SA-Hydra 4.1.8

The following are components that were part of the Splunk Add-on for NetApp Data ONTAP until version 3.0.1 and are now available as individual packages:

- TA-ONTAP-FieldExtractions 3.0.2 (Splunk Add-on for NetApp Data ONTAP Extractions)
- SA-ONTAPIndex 3.0.2 (Splunk Add-on for NetApp Data ONTAP Indexes)

Source types for the Splunk Add-on for NetApp Data ONTAP

The Splunk Add-on for NetApp Data ONTAP collects API data from NetApp storage controllers running Data ONTAP in 7-mode or cluster mode. It collects performance data about specific inventory objects and data about the configuration of your NetApp storage infrastructure. We collect logs on NetApp filers that contain basic information about their operation. This gives you the visibility you need into the health and state of your storage infrastructure enabling you to better manage it.

API data collection is managed by the Hydra scheduler working with the data collection nodes. The exception to this is the collection of syslog data from the filers.

The data we collect

The following NetApp data types are collected by the app:

Data source	Data type	Description
API	**Inventory data**	This data is collected from the Net App filers in 7-mode and Cluster mode and contain information about specific object instances. These objects are volume, disk, LUN, aggregate, vFiler, QTree, and Quota.
API	**Performance data**	Performance data is collected from the following NetApp filer objects in 7-mode and Cluster mode: volume, disk, LUN, aggregate, vFiler, QTree, and Quota. Performance counters collect data for performance objects.
API	**Options data**	This add-on collects 7-mode options data and Cluster cifs-options data.
API	**EMS data**	The app collects details of critical activities from the NetApp filer Event Management System (EMS).
Syslog	**NetApp filer logs**	These are log files generated by the NetApp filer in 7-mode and cluster mode. This data is collected by configuring the NetApp filers to send the logs to a syslog server (over the network).

Sourcetype	Eventtype	Tags
`ontap:perf`	Performance	performance, storage
`ontap:system`	Storage	storage
`ontap:volume`	Storage	storage
`ontap:disk`	Storage	storage
`ontap:aggr`	Storage	storage
`ontap:lun`	Storage	storage
`ontap:vserver`	Storage	storage
`ontap:qtree`	Storage	storage
`ontap:quota`	Storage	storage
`ontap:cifsoptions`	Storage	storage
`ontap:options`	Storage	storage
`ontap:ems`	Storage	storage
`ontap:nfsexports`	Storage	storage
`ontap:cluster`	Storage	storage

Common Information Model compliance

The Splunk Add-on for NetApp Data ONTAP supports the following event categories in the CIM:

- Inventory
- Performance

Note: The Splunk Add-on for NetApp Data ONTAP does not extract CIM data for **storage** and **cpu** objects of the **performance** data model.

The Common Information Model is available as an Add-on that implements the CIM tables as **data models**. You can download the Splunk Common Information Model Add-on (Splunk_SA_CIM) from Splunk Apps. For more information on the Splunk Common Information Model Add-on, see the "Common Information Model Add-on" topic in the Splunk Enterprise documentation. See also the Splunk documentation on how to "Understand and use the Common Information Model" in the Knowledge Manager Manual.

You can use the data models available in the Splunk Common Information Model Add-on in two ways:

- You can use them to test whether your fields and tags have been normalized correctly.
- After you've verified that your data is normalized you can use the models to generate reports and dashboard panels via Pivot.

The CIM enables you to identify common events across different technologies and, using the CIM, you can build a variety of specialized searches across the datasets that have been mapped to event categories relevant to the underlying technologies. Splunk_SA_CIM is a repository of data models that can be used with Splunk apps and Splunk 6.0 or later. The CIM identifies the fields that must be present in the data for the dashboards to work, and the tags that need to be assigned to the data for the process to work correctly.

For information about the fields in these event categories, read "Standard fields and event category tags" in the Splunk Knowledge Manager manual.

When you add sourcetypes for your data to the Splunk Add-on for NetApp Data ONTAP, refer to the Splunk Enterprise CIM documentation to ensure that you follow the requirements for data processing to CIM standards.

Key performance counters

You can collect data for each performance object in your storage system. We monitor the performance of your storage systems by collecting the key performance counters for your storage devices so that you can be proactive in configuring your system to meet your storage demands and troubleshooting your performance issues. This enables you to identify and diagnose problems early.

Example using performance counters for the Volume object

We use performance counters in some of the searches that power the dashboards in the Splunk Add-on for NetApp Data ONTAP. For example, in the Volume Detail dashboard we use the latency values (average, other, read, and write) to chart the latency values over time for reads to the volume, writes to the volume, average latency for all operations on the volume, and the average time for other operations on the volume. All operations are reported in milliseconds. Look at the "Selected Volume Latency (ms)" panel in the Volume Detail dashboard to see the results of the search.

```
sourcetype=ontap:perf source=VolumePerfHandler host="host_name" objname="volume_name" | timechart
first(eval(avg_latency_average/1000)) as avg_latency_average first(eval(other_latency_average/1000)) as
other_latency_averagefirst(eval(write_latency_average/1000)) as write_latency_average
first(eval(read_latency_average/1000)) as read_latency_average by objname
```

You can also create your own custom searches using the storage performance counters. Run your search in the Search bar in Splunk. For example, you can use the performance counter "Average Volume Latency" in a search to collect the average latency of all of the operations on the volume and then display the last received value by host and volume name.

An example of a search that can do this is:

```
index=ontap sourcetype=ontap:perf source=VolumePerfHandler avg_latency_average=* | rename objname as
volume_name | stats last(avg_latency_average) by host,volume_name
```

The result is a table that displayed the host names, the volume name on the host, and the last latency values.

Release notes for Splunk Add-on for NetApp Data ONTAP

Version 3.0.3 of the Splunk Add-on for NetApp Data ONTAP was released on July 12th, 2022.

What's New

Update	Description
Added triggers stanza for custom configuration files	To avoid unnecessary restarts of the Splunk platform, app.conf file was updated with a [triggers] stanza and a reload setting for custom configuration file.

Splunk Add-on for NetApp Data ONTAP Indexes (SA-ONTAPIndex) and Splunk Add-on for NetApp Data ONTAP Extractions (TA-ONTAP-FieldExtractions) packages have been removed from the add-on package and published as an independent apps with version 3.0.2 in order to support self-service installation in the cloud environment.

See Upgrade the Splunk Add-on for NetApp Data ONTAP to upgrade or see Installation overview to install the add-on.

See the fixed issues and known issues of these release notes for product updates.

Fixed Issues

This version of the Splunk Add-on for NetApp Data ONTAP fixes the following issues. If no issues appear below, no issues have yet been reported.

Known Issues

This version of the Splunk Add-on for NetApp Data ONTAP has the following reported known issues and workarounds. If no issues appear below, no issues have yet been reported.

Date filed	Issue number	Description
2021-06-01	NETAPP-1027	Drill-down not working in Event viewer panels in Hydra Framework in Splunk 8.2.0
2017-03-08	NETAPP-801	Need to extract "ontap_version" field for NETAPP cluster mode having API version higher than v1.30.

Release history for Splunk Add-on for NetApp Data ONTAP

Latest release

The latest version of the Splunk Add-on for NetApp Data ONTAP is version 3.0.3. See Release notes for the Splunk Add-on for NetApp Data ONTAP for the release notes of this latest version.

Version 3.0.2

Update	Description
Self-service add-on installation compatibility	Splunk Add-on for NetApp Data Ontap is now compatible with self-service add-on installation in Cloud environments.
jQuery 3.5 compatibility	The Splunk Add-on for NetApp Data ONTAP now uses jQuery v3.5.0. The add-on uses jQuery v3.5 in Splunk Enterprise version 8.2 or higher. This makes the add-on more secure by fixing known cross-site scripting (XSS) related vulnerabilities as well as vulnerabilities created by object prototype pollution.
Hydra troubleshooting dashboards in the Extractions package	The Hydra troubleshooting dashboards Hydra Framework Status and Hydra Scheduler Status have been added to the TA-ONTAP-FieldExtractions package to remove the dependency of SA-Hydra from the search head. The SA-Hydra package is no longer required on the search head.

Update	Description
Removal of SA-VMNetAppUtils module from the add-on package	Splunk Add-on for NetApp Data ONTAP does not use any KO or modules from SA-VMNetAppUtils package. This module is no longer required and is removed from the add-on package. If you are using the module, then you can keep the module as is.

Splunk Add-on for NetApp Data ONTAP Indexes (SA-ONTAPIndex) and Splunk Add-on for NetApp Data ONTAP Extractions (TA-ONTAP-FieldExtractions) packages have been removed from the add-on package and published as independent apps with version 3.0.2 in order to support self-service installation in the cloud environment.

Version 3.0.1

In Splunk Add-on for NetApp Data ONTAP version 3.0.1, occurrences of biased terms such as master, slave, blacklist, and whitelist have been replaced with appropriate non-biased terms. The occurrences of biased terms that are Splunk platform references or present in the third-party library have not been removed.

If you are using per_panel_filter, ppf_subsearch, ppf_subsearch_dm, and per_panel_filter_lookup macros of the SA-VMNetAppUtils package in your custom dashboard or in the saved searches, then you must update the value of the filter field in the lookup file where you're using with these macros. All static variables values for ppf_lookup_type, ppf_filter have been updated from blacklist to denylist, and from whitelist to allow list.

This version of the Splunk Add-on for NetApp Data ONTAP has the following reported known issues and workarounds. If no issues appear below, no issues have yet been reported.

Date filed	Issue number	Description
2020-09-02	NETAPP-937	There's an invalid key error on Splunk 7.x because the Addon uses the Python 3 interpreter by default.
2017-03-08	NETAPP-801	Need to extract "ontap_version" field for NETAPP cluster mode having API version higher than v1.30.

Version 2.1.6

Starting in version 2.1.5 of the Splunk App for NetApp Data ONTAP, the `SA-Utils` package required on the search head, scheduler and DCNs has been replaced with `SA-VMWNetAppUtils`. For more information on upgrading from a previous version of the Splunk App for NetApp Data ONTAP, see the upgrade steps in the Splunk App for NetApp Data ONTAP manual.

NetApp changed the default behavior of the API `perf-object-instance-list-info-iter` and objectname "system", starting with the NETAPP API v1.30. The below returns aggregated data instead of node level data. Because of this, the below fields are not returned starting from API v1.30.

- `compile_flags`
- `hostname`
- `node_name`
- `node_uuid`
- `ontap_version`
- `process_name`
- `serial_no`
- `system_id`
- `system_model`

Fixed Issues

Date resolved	Issue number	Description
2017-03-09	NETAPP-796	NetApp changed the default behavior of the API "perf-object-instance-list-info-iter" and objectname "system", starting with the NETAPP API v1.30

Known Issues

Date	Issue number	Description
2017-05-03	NETAPP-821	Fields are not returned in API response starting from v1.30.

Date filed	Issue number	Description
2017-09-11	NETAPP-831	Update SA-Hydra version from 4.0.5 to 4.0.6 and SA-VMNetAppUtils version from 1.0.1 to 1.0.2
2017-03-08	NETAPP-801	Need to extract "ontap_version" field for NETAPP cluster mode having API version higher than v1.30.

Installation and Configuration

Hardware and software requirements

Splunk Enterprise requirements

- If you're using the Splunk Add-on for NetApp Data ONTAP for configuration or data collection, install the add-on on the scheduler and data collection node in a Linux x64 environment. See "System requirements" in the Splunk Enterprise *Installation Manual*.
- If you're using the Splunk Add-on for NetApp Data ONTAP as a search time knowledge object, install the add-on on the search head indexer, which is platform independent.
- Splunk Enterprise 8.0.x, 8.1.x, 8.2.x, and 9.0.0
- A valid Splunk Enterprise license that supports approximately 300 MB to 1GB of data per filer per day.
- A Splunk Enterprise server or forwarder with network access to the NetApp storage controllers.

Distributed Collection Scheduler requirements

These supporting add-ons support the Distributed Collection Scheduler in the Splunk Add-on for NetApp Data ONTAP.

- SA-Hydra version 4.1.6.

Supported NetApp versions

The following table displays the versions of the Splunk Add-on for NetApp Data ONTAP that have been tested and proven to be compatible with the below versions of the ONTAP line of products.

Splunk Add-on for NetApp Data ONTAP version	Splunk Add-on for NetApp Data ONTAP Indexes version	Splunk Add-on for NetApp Data ONTAP Extractions version	Splunk App for NetApp Data ONTAP version	Splunk Enterprise version	NetAppÂ® Data ONTAPÂ® 7-Mode version	NetAppÂ® Data ONTAPÂ® Cluster Mode version
3.0.2, 3.0.3	3.0.2	3.0.2	2.1.91	8.0.x, 8.1.x, 8.2.x, 9.0.0	up to 8.3	up to 9.9.1

Splunk Enterprise supports NetAppÂ® DATA ONTAP on NetApp V-series and FAS controllers.

Browser support

Splunk Add-on for NetApp Data ONTAP supports the browser versions listed below:

- Firefox (latest)
- Safari (latest)
- Chrome (latest)

Requirements for installing Splunk Add-on for NetApp ONTAP with other add-ons in the same environment

The following requirements apply to installing Splunk Add-on for NetApp ONTAP and Splunk Add-on for VMware in the same environment:

Splunk Add-on for NetApp ONTAP version	Splunk Add-on for VMware version	Can DCS be installed on the same machine?	Can DCN be installed on the same machine?
3.0.0 or later	3.4.6 or later	No	No
2.1.91 or before	3.4.5 or before	Yes	No

The following requirements apply to installing Splunk Add-on for NetApp ONTAP and Splunk Add-on for VMware Metrics in the same environment:

Splunk Add-on for NetApp ONTAP	Splunk Add-on for VMware Metrics version	Can DCS be installed on the same machine?	Can DCN be installed on the same machine?
3.0.0	4.0.0 or later	Yes	No
3.0.0	1.0.0, 1.1.0 or 1.1.1 (Splunk VMware Add-on for ITSI)	No	No

Splunk Add-on for NetApp Data ONTAP data volume requirements

Splunk Add-on for NetApp Data ONTAP requires a license that can collect:

- performance data at a volume of 300MB to 1GB per filer per day
- syslog data at a volume of 100MB

The number of volumes and disks in your NetApp environment directly impact your data volume.

When you have the app up and running, navigate to the App Data Volume view to see the volume of data it is indexing in your environment. From the App menu, select **Settings**, then **App Data Volume**. You can see:

- The total quantity of data indexed over a 24 hour time period
- A breakdown of the type of data, and the volume of each type

Splunk data collection node resource requirements

At a minimum, a single data collection node requires:

- 4 cores - 4 vCPUs or 2 vCPUs with 2 cores with a reservation of 2 GHz
- 6GB memory with a reservation of 1 GB
- 4-10 GB of disk space

At these requirements, one data collection node can collect from 20 filers.

Software requirements

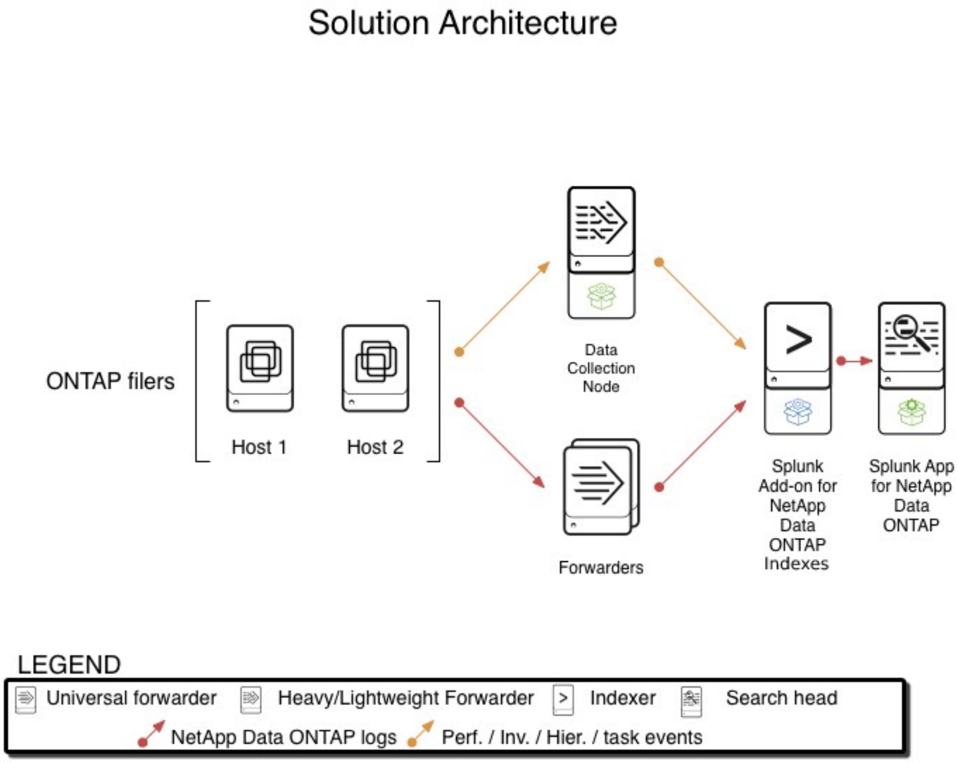
A single data collection node requires:

- A version of CentOS or RedHat Enterprise Linux (RHEL) that is compatible with one of the following:
    - ◊ Splunk Enterprise 8.0.0 or later.

- A Splunk Enterprise heavy forwarder or light forwarder, version 7.3.0 or later. This is a minimum Splunk requirement for the Splunk App for NetApp Data ONTAP. You cannot use a universal forwarder.

Installation overview

The Splunk Add-on for NetApp Data ONTAP works with NetAppÂ® Data ONTAP to collect granular performance, log, and event data about the storage layer and bring it into Splunk. You can then use this data and correlate it with other data in your environment.



Use the following table when installing the Splunk Add-on for NetApp Data ONTAP onto your Splunk platform deployment. It shows what apps are required and where to install them.

> The Splunk Add-on for NetApp Data ONTAP no longer depends on SA-VMNetAppUtils. The SA-VMNetAppUtils module is no longer part of the Splunk Add-on for NetApp Data ONTAP. If you're using any knowledge objects from SA-VMNetAppUtils independent from the add-on, then do not remove the module from the search head when upgrading the add-on from version 3.0.1.

Splunk Add-on for NetApp Data ONTAP deployment table

Splunkbase Name	Component	Search Head	Data Collection Node	Indexer	Scheduler
Splunk Add-on for NetApp Data ONTAP	Splunk_TA_ontap SA-Hydra		X		X
Splunk Add-on for NetApp Data ONTAP Indexes	SA-ONTAPIndex			X	
Splunk Add-on for NetApp Data ONTAP Extractions	TA-ONTAP-FieldExtractions	X			

> The SA-Hydra package from Splunk Add-on for NetApp Data ONTAP version 3.0.1 was required on the search head to access Hydra troubleshooting dashboards, Hydra Framework Status and Hydra Scheduler Status. In version 3.0.2, these dashboards are added to the TA-ONTAP-FieldExtractions package. Therefore, the SA-Hydra package is no longer required on the search head.

Splunk Add-on for NetApp Data ONTAP deployment table with Splunk App for NetApp Data ONTAP installed

Splunkbase Name	Component	Search Head	Data Collection Node	Indexer	Scheduler
Splunk Add-on for NetApp Data ONTAP	Splunk_TA_ontap SA-Hydra		X		X
Splunk App for NetApp Data ONTAP	splunk_app_netapp	X			
Splunk Add-on for NetApp Data ONTAP Indexes	SA-ONTAPIndex			X	
Splunk Add-on for NetApp Data ONTAP Extractions	TA-ONTAP-FieldExtractions	X			

Install the Splunk Add-on for NetApp Data ONTAP

Install the Splunk Add-on for NetApp Data ONTAP for use with the Splunk App for NetApp Data ONTAP and the Storage Module for Splunk IT Service Intelligence. See the installation sections for the Splunk App for NetApp Data ONTAP and Splunk IT Service Intelligence for more information.

Deployment Compatibility

This table provides information about the Splunk Add-on for NetApp ONTAP compatibility with Splunk distributed deployment features.

Distributed Deployment Feature	Supported	Notes
Search Head Clusters	Yes	Install the TA-ONTAP-FieldExtractions package to get the search-time field extractions on your Search Head. Install the Splunk Add-on for NetApp Data ONTAP Extractions package on your deployer before pushing the package from the deployer to Search Head. You do not need to install components Splunk_TA_ontap and SA-ONTAPIndex on your deployer.
Indexer Clusters	Yes	Install the SA-ONTAPIndex package to define the indexes used by Splunk Add-on for NetApp Data ONTAP. Install the component SA-ONTAPIndex from the Splunk Add-on for NetApp Data ONTAP Indexes package onto your cluster manager to deploy the Splunk Add-on for NetApp Data ONTAP packages.
Deployment Server	Yes	If you use a deployment server, install the Splunk Add-on for NetApp Data ONTAP onto your deployment servers. See About deployment server and forwarder management to learn more about managing your deployment servers.

Follow the installation steps that suit your deployment type.

Single-instance deployment

A single-instance deployment of the Splunk platform contains indexers and search heads on a single host. Here's how to install the add-on for a single-instance deployment.

1. Download the below add-ons from Splunkbase.
    1. Splunk Add-on for NetApp Data ONTAP
    2. Splunk Add-on for NetApp Data ONTAP Indexes
    3. Splunk Add-on for NetApp Data ONTAP Extractions
2. Extract the packages in the .tgz file in downloaded add-on builds to `$SPLUNK_HOME/etc/apps`.
3. Verify that all of the installation components exist in the `$SPLUNK_HOME/etc/apps` folder.
4. Restart your Splunk platform instance.

Search head cluster environment

Versions 2.1.5 and later of the Splunk Add-on for NetApp Data ONTAP supports search head clustering environments. Perform the following steps to set up the add-on in a search head cluster deployment. This configuration improves the overall performance of the Splunk Add-on for NetApp Data ONTAP in a search head cluster environment.

For an overview of search head clustering, see Search head clustering architecture in the Splunk Enterprise *Distributed Search* manual.

Prerequisites

The following are prerequisites for installing the add-on in a search head cluster environment:

- You have a minimum of 3 Splunk Enterprise instances to serve as search head cluster members and one additional instance that serves as a deployer which you use to distribute apps and updated configurations to the cluster members.
- The scheduler must be deployed on a dedicated search head and not on any individual search head in the search head cluster.
- Each search head cluster member must be fresh install of Splunk Enterprise and not re-purposed instance.

- You have migrated your settings from a search head pool to a search head cluster. For more information, see Migrate from a search head pool to a search head cluster in the Splunk Enterprise *Distributed Search* manual.
- You have a licensed version of Splunk Enterprise installed and running in your environment.

Install your search head cluster

Splunk Add-on for NetApp Data ONTAP version 2.1.5 and higher supports search head clustering .

See Deploy a search head cluster in the Splunk Enterprise *Distributed Search* manual for more information on how to install, configure, and deploy a search head cluster.

Install and deploy the Splunk Add-on for NetApp Data ONTAP on your search head cluster

Complete the following steps to download, install, and deploy the Splunk Add-on for NetApp Data ONTAP on the tiers of your search head cluster.

You must use the search head cluster deployer to distribute your configurations across your set of search head cluster members. See Use the deployer to distribute apps and configuration updates in the Splunk Enterprise *Distributed Search* manual.

Install on the scheduler and data collection nodes

1. Download the Splunk Add-on for NetApp Data ONTAP from Splunkbase.
2. Extract the packages present in the downloaded build to the `$SPLUNK_HOME/etc/apps` directory on the forwarder.
3. Restart the Splunk services.

Install on Indexers

1. Download the Splunk Add-on for NetApp Data ONTAP Indexes from Splunkbase.
2. Extract the packages present in the downloaded build to the `$SPLUNK_HOME/etc/master-apps` directory on the cluster master.
3. Apply the changes to the indexers from the cluster master using the following command:

```
./splunk apply cluster-bundle -auth <username>:<password>
```

Install on search heads

1. Download the Splunk Add-on for NetApp Data ONTAP Extractions from Splunkbase.
2. Extract the packages present in the downloaded build to the `$SPLUNK_HOME/etc/shcluster/apps` directory on the deployer.
3. Apply the changes to the search heads from the deployer using the following command:

```
./splunk apply shcluster-bundle -target <URI>:<management_port> -auth <username>:<password>
```

Distributed installation

For larger environments where data originates from many machines and where many users need to search the data, you can separate the indexing and searching functions. In this type of distributed search deployment, each indexer indexes data and performs searches across its own indexes. A Splunk Enterprise instance dedicated to search management, called the search head, coordinates searches across the set of indexers, consolidating the results and presenting them to the user. For more information about distributed search, see About distributed search in the *Distributed search* manual.

Complete the following steps for the specific components:

Install on DCN

1. Download the Splunk Add-on for NetApp Data ONTAP from Splunkbase.
2. Extract the packages present in the downloaded build to the $SPLUNK_HOME/etc/apps directory on the DCN.
3. Apply the changes to the DCN by restarting the Splunk services on the DCN.

Install on scheduler

1. Download the Splunk Add-on for NetApp Data ONTAP from Splunkbase.
2. Extract the package present in the downloaded build to the `SPLUNK_HOME/etc/apps directory` on the DCS.

Apply the changes to the DCS by restarting the Splunk services on the DCS.

Install on indexers

1. Download the Splunk Add-on for NetApp Data ONTAP Indexes from Splunkbase.
2. Extract the packages present in the downloaded build to the `SPLUNK_HOME/etc/apps` directory on the indexers.
3. Apply the changes to the indexers by restarting the Splunk services on the indexers.

Install on search heads

1. Download the Splunk Add-on for NetApp Data ONTAP Extractions from Splunkbase.
2. Extract the package present in the downloaded build to the `SPLUNK_HOME/etc/apps` directory on the search heads.
3. Apply the changes to the search heads by restarting the Splunk services on the search heads.

Cloud environment

Complete the following steps to install the add-on in a cloud environment. See the NetApp Data ONTAP Installation overview and review the deployment diagram if you haven't yet.

The scheduler and data collection node (DCN) instances for the add-on must be on-premise. The indexer and search tead tier can be part of the cloud environment. See the previous section to set up the add-on on the scheduler and data collection node.

Complete the following steps to install the required add-on packages on the indexer and search heads present in the cloud environment:

1. Login to your search head.
2. On the Splunk Web home page, click "Find More Apps".
3. Search for the following add-ons:.
    1. Splunk Add-on for NetApp Data ONTAP Indexes
    2. Splunk Add-on for NetApp Data ONTAP Extractions
4. Click **Install**.
5. Review the confirmation message.
6. Click **Continue**.
7. Enter your Splunk.com login credentials.
8. Read and accept the login disclaimer
9. Click **Login and Download**.
10. On the **App Management** page, review the installed apps.

Install and configure data collection nodes

You must have at least one data collection node installed and running in your environment to collect ONTAP API data. You can build a data collection node and configure it as a physical machine or as a VM image to deploy specifically for your environment.

install a Splunk heavy forwarder or light forwarder, version 7.3.0 to 9.0.0 on the host that will be your data collection node. You cannot use a Splunk Universal Forwarder for it because Python is required. This is a minimum Splunk requirement for the Splunk App for NetApp Data ONTAP. A data collection node requires that you have a Splunk supported version of CentOS or RedHat Enterprise Linux (RHEL) that is supported by Splunk version 6.3.1 or later. For search head cluster environments, data collection nodes must still be dedicated to a separate search head for scheduling.

Follow the steps below to build a physical data collection node or a VM data collection node. To build a data collection node VM, follow the guidelines set by your specific virtualization solution to create the virtual machine and deploy it in your environment.

Build a data collection node

1. Install a CentOS or RedHat Enterprise Linux version that is supported by Splunk Enterprise version 7.3.0 to 9.0.0.
    1. For system compatibility information, see Splunk data collection node resource requirements in this manual.
2. Install Splunk Enterprise version 7.3.0 to 9.0.0 configured as light or heavy forwarder (Python is required). **Note:** you cannot use a Splunk universal forwarder.
3. Install the app components. Get the file `splunk_add_on_for_netapp-<number>.tgz` and put it in `$SPLUNK_HOME/etc/apps`.
4. Extract this file. It automatically extracts into the `$SPLUNK_HOME/etc/apps` directory.
5. On the data collection node you need the following components: SA-Hydra and Splunk_TA_ontap in `$SPLUNK_HOME/etc/apps`. Do not install splunk_app_netapp in a data collection node.
6. Check that firewall ports are enabled. The data collection node communicates, by default, with splunkd on port 8089. It communicates with the scheduling node, by default on port 8008. These are the default ports. For more information on configuring firewall ports, see Network settings in this manual.
7. Set up forwarding to the port on which the Splunk indexer(s) is configured to receive data. See Enable a receiver in the *Forwarding Data* manual.
8. Change the default password using the CLI for this forwarder. The default password for Splunk's `admin` user is `changeme`. Be sure to change the value of the password to something other than `changeme`.
    ```
    ./splunk edit user admin -password 'newpassword' -role admin -auth admin:changeme
    ```
9. Restart Splunk.
10. After deploying the collection components, add the forwarder to your scheduler's configuration. To do this, see Collect data from your environment in this manual.

Set static IP addresses

While not required, setting a static IP address for the data collection node is recommended. The data collection node's IP address can vary over time when using DHCP (dynamic addressing), causing unexpected results. Connecting to a specific collection node can be difficult (especially if DNS is down). You can connect to the data collection node to perform maintenance or to determine which collection node is sending data.

Change the NTP server pool list

The Network Time Protocol (NTP) is used to synchronize a computer's time with another reference time source. Most *Nix systems give you the ability to set up or change time synchronization. You can change the NTP servers that your data collection node uses by editing the `/etc/ntp.conf` file.

The default values for the servers in `/etc/ntp.conf` are:

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
server 0.centos.pool.ntp.org
server 1.centos.pool.ntp.org
server 2.centos.pool.ntp.org
```

To use different NTP servers, replace the default values in the file with your specific values. Restart ntpd for the changes to take effect.

```
sudo service ntpd restart
```

Disable NTP on the data collection node

If you do not have access to the internet (for example, you operate behind a firewall that precludes access to the Internet) you can disable NTP on the data collection node.

Upgrade from the Splunk App NetApp Data ONTAP versions 2.1.4 and earlier

To upgrade your deployment from a versions 2.1.4 and earlier of the Splunk App NetApp Data ONTAP, see the Upgrade to Splunk App for NetApp Data ONTAP 2.1.5 section of the Splunk App for NetApp Data ONTAP manual.

Configure inputs

Configure receivers for ONTAP data

After installation, set up receiving on each of your indexers. Receivers, by convention, listen on port 9997, but any unused port is permitted. For more information see Set up receiving in the Splunk Forwarding data manual.

Configure Splunk to receive syslog data

Use a data collection node as the collection point for syslog data as it has **Splunk_TA_ontap** installed and the data input is set up. When you have installed the Splunk Add-on for NetApp Data ONTAP on the selected data collection node, enable the ontap:syslog data input by performing the below steps:

1. Copy the below stanza from `$SPLUNK_HOME/etc/apps/Splunk_TA_ontap/default/inputs.conf` to `$SPLUNK_HOME/etc/apps/Splunk_TA_ontap/local/inputs.conf`:

   ```
   #[udp://514]
   #index = ontap
   #sourcetype = ontap:syslog
   #connection_host = dns
   #disabled = 0
   ```
2. Uncomment this stanza in the local version of inputs.conf.

In very large environments, if you see a degradation in performance of your data collection node you can manually split the collection of your syslog data across multiple data collection nodes.

You can also use a dedicated forwarder or use the indexer that is connected to the data collection node as the collection point. In all cases, follow standard Splunk practices to configure Splunk to receive syslog data. Check that:

- Splunk is listening on UDP port 514.
- The sourcetype is set to `ontap:syslog` in the `inputs.conf` file.
- Splunk_TA_ontap is installed on the machine receiving syslog.

If you currently collect syslog data from the NetApp filers using a Splunk forwarder, you can continue to use the setup you have in your environment. Check that the forwarder receiving syslog is configured to send the data to the same indexers as the data collection node.

System log (syslog) management is important for troubleshooting performance problems across your network. Configure system log forwarding from NetApp to Splunk separately for your 7-mode and cluster mode filers. Log forwarding is done on the command line in your NetApp environment to forward to a Splunk forwarder. The forwarder must have network access to the storage device and be configured to listen on UDP port 514. Read the topic "Get data from TCP and UDP ports" in the Getting Data In manual for more information.

Turn on logging on data collection nodes

Turning on logging on the data collection node when you create the node assists in troubleshooting data collection issues. The collected data counts against your Splunk license.

1. Navigate to your data collection node.
2. Navigate to the `SA-Hydra` directory, and create a `local` directory.
3. Copy the `outputs.conf` file from `SA-Hydra/default/` move it to `SA-Hydra/local/`.
4. Edit the `SA-Hydra/local/outputs.conf` file to uncomment the following lines:

```
[tcpout]
forwardedindex.3.whitelist = _internal
```

Configure timezones in syslog data

Ensure that the clock and timezone settings for your Splunk platform environment and your ONTAP servers agree so as to ensure accurate timestamping. In your Splunk platform, time offsets can cause indexing issues with defined data types. This is specifically true in the Splunk App for NetApp Data ONTAP for performance searches that use report acceleration. If the timezone information is not set correctly, your Splunk platform may incorrectly apply a timestamp and potentially exclude events from indexing. A light forwarder (LF) or universal forwarder (UF) do not parse events to get a timestamp. As a NetApp administrator, use NTP on your filers to check that the timezone settings on your ONTAP servers match the timezone information on your Splunk indexer(s).

Configure your NetApp environment to send syslog data to Splunk

In both 7-mode and in cluster mode, syslog is forwarded from your NetApp storage systems to Splunk by default on UDP port 514.

Configure syslog on 7-mode filers

1. Log in to the NetApp filer with the correct permissions.
2. To configure forwarding, on the command line enter the following, where forwarder is the IP address or DNS name of the receiving host:

```
wrfile -a /etc/syslog.conf *.* @<forwarder>
```

Configure syslog forwarding on Cluster mode

In cluster mode there are many types of events, one of which is a syslog event. You can use specific Data ONTAP commands in the event family for managing these events. See the complete list of "Commands for managing events" in the NetApp online support documentation.

Configuring syslog in cluster mode is a two step process. First create a destination to where you will send the event. Once this is done you can forward the syslog event. You can forward to multiple forwarders, but you must specify a name for each one.

ONTAP Cluster Mode 9.0 and above

1. Log in to the NetApp filer with the correct permissions.
2. On the command line, set up the destination for the event, where `<machine_name>` is the IP address or DNS name of the receiving host:
   ```
   event notification destination create -name <name> -syslog <Forwarder_IP>
   ```
3. Filter forwarded data. You can forward all of the data from the cluster or you can forward a select set of data.
   1. Create filter `event filter create -filter-name <filter_name>`
   2. Forward syslogs using filters `event notification create -filter-name <filter_name> -destinations <name_of_destination>`
   3. View event destinations `event notification destination show`
4. Add a rule to the created filter in order to forward events.
   ```
   event filter rule add -filter-name <filtername> -type include -position <rule position>
   -severity <severity type>
   ```

ONTAP Cluster Mode 8.x and below

1. Log in to the NetApp filer with the correct permissions.
2. On the command line, set up the destination for the event as follows, where `<machine_name>` is the IP address or DNS name of the receiving host:
   ```
   event destination create -name int_fwd -syslog <machine_name>
   ```
3. Specify exactly what you want to forward. You can forward all of the data from the cluster or you can forward a select set of data. In this command you add the destination(s) established in the previous step to the event route. In this example we forward all of the data.
4. Filter the data you want to forward, and forward the data using this command:
   ```
   event route add-destinations -destinations int_fwd -messagename all
   ```

See the NetApp documentation, on "Managing event messages" for more detailed information.

Configure data collection intervals

The Splunk Add-on for NetApp Data ONTAP collects metrics for performance data and inventory data. Collection intervals are set in the `$SPLUNK_HOME/etc/apps/Splunk_TA_ontap/default/ta_ontap_collection.conf` file. The following two keys, **megaperf_interval** and **megainv_interval**, included in the default stanza of this file are used to set the intervals for data collection. The value that you assign to the interval reflects how you want to collect data in your environment. Use the number of objects (such as disk, volume, lun, qtree, or any other "inventory" object) on the filer to determine the interval settings for **megaperf_interval** and the **megainv_interval** for each filer. The most critical interval is the **megaperf_interval**. This interval governs the granularity of the performance data you collect and the total number of events coming into the system.

To collect data at the most granular level you must know the minimum performance interval. The minimum performance interval for performance data for this add-on is on average 0.1 to 0.2 seconds per object on the filer, given that no network issues impact collection.

For example, to calculate the recommended **megaperf_interval** in seconds for 3000 volumes, multiply the number of volumes by the minimum performance interval (0.2). This gives an interval value of 600 seconds.

The volume of data we collect for the **megainv_interval** is less than that of the **megaperf_interval** and the data is less frequent. We recommend a collection interval value that is 5 to 20 times the performance interval, so long as the interval is set to a value less than 60 minutes. To schedule performance and inventory collection on the same intervals, use the guidelines described above for collecting the data. Aggressive collection of inventory data (on the same frequency with which performance data is being collected) is not recommended.

The following is an example of the interval settings in the `ta_ontap_collection.conf` file

```
[default]
megaperf_interval = 60
megaperf_expiration = 55
megainv_interval = 600
megainv_expiration = 595
```

Distribute API requests across multiple data collection nodes

Distribute API requests across multiple data collection nodes (DCNs) to improve collection processing speed and to reduce collection fails. See the below example to use 2 DCNs to distribute performance and inventory collection.

Use two data collection nodes and distribute perf and inventory collection

1. Create two data collection nodes.
2. Navigate to the first DCN, and connect to NetApp Filer 1
3. Navigate to the `default` and copy the inputs.conf file.
4. Create a `local` directory and move the copied `inputs.conf` file to the `local` directory.
5. In the `local/inputs.conf` file, change the `[default]` stanza tasks from `megainv, megaperf` to `megaperf`.
   Example

   ```
   [default]
   tasks = megaperf
   ```
6. Navigate to the second DCN, and connect to NetApp Filer 1
7. Navigate to the `default` and copy the inputs.conf file.
8. Create a `local` directory and move the copied `inputs.conf` file to the `local` directory.
9. In the `local/inputs.conf` file, change the `[default]` stanza tasks from `megainv, megaperf` to `megainv`.
   Example

   ```
   [default]
   tasks = megainv
   ```

How to limit performance data collection

To reduce the volume of ONTAP performance data coming into the add-on, or to reduce the number of tasks that expire before they can complete, you can change the interval setting in the `$SPLUNK_HOME/etc/apps/Splunk_TA_ontap/default/ta_ontap_collection.conf` file. This affects the frequency with which ONTAP performance data is collected. Changing the collection interval also has an effect on the granularity of the ONTAP data you collect.

To change interval settings, create a local version of the file, if it does not already exist, (`$SPLUNK_HOME/etc/apps/Splunk_TA_ontap/local/ta_ontap_collection.conf`) and specify the changes here.

On the search head that runs the scheduler:

1. Edit the file `$SPLUNK_HOME/etc/apps/Splunk_TA_ontap/local/ta_ontap_collection.conf`. If it does not exist, create a new file.
2. Include the following stanza that affects ONTAP performance data collection:
   ```
   [default]
   megaperf_interval = 60
   megaperf_expiration = 55
   megainv_interval = 600
   megainv_expiration = 595
   ```
3. Restart Splunk.

Keep the value that you assign to expiration 5 to 10 seconds lower than the value you assign to the interval.

Set up the Splunk Add-on for NetApp Data ONTAP to collect data from your ONTAP environment

Step 1: Configure user roles

There are two default user roles defined in the Splunk Add-on for NetApp Data ONTAP and the Splunk App for NetApp Data ONTAP:

- The **splunk_ontap_admin** role: This role gives you permission to configure the Splunk Add-on for NetApp Data ONTAP for data collection.
- The **splunk_ontap_user** role: This role gives you permission to use the add-on. It does not give you permission to configure the add-on.

Configure roles for the users of the add-on on the following components:

- Scheduler (If using a separate scheduler)
- Search head (or the combined indexer and search head)

Assign roles to each users

1. Log in to Splunk Web and enter the IP address and port number of the OS hosting your search head and/or scheduler: `http://<ipaddress>:8000/`
2. Select the Splunk Add-on for NetApp Data ONTAP from the Apps menu, and navigate to the **Collection Configuration** page. If this is your first time installing the app, then you are automatically redirected to the **Setup** page. Accept all of the default settings on the **Setup** screen, then click **Save**. For most installations the default settings work.
3. In **Settings**, select **Users and authentication: Access controls**, then select **Users**.
4. Give the admin user the **splunk_ontap_admin** role so that the admin can run scheduled searches. Add **splunk_ontap_admin** to the "admin" account.
5. Provide **admin_all_objects** capability to the splunk_ontap_admin role.
   1. Go to the **Settings**>**Access controls**>**Roles**>**splunk_ontap_admin**.
   2. Add **admin_all_objects** capability.
   3. click **Save**.

Step 2: ONTAP Collection Configuration

In Splunk Web on your search head, select **Add-on for ONTAP** from the app menu,. This brings you to the Splunk Add-on for NetApp Data ONTAP **Collection Configuration** dashboard.

Use the ONTAP Collection Configuration dashboard as a single point of configuration for ONTAP servers instead of having to manage the credentials for each machine individually. If your servers have the same administration credentials (admin/password), then realm based access simplifies the process of adding ONTAP servers to the Splunk Add-on for NetApp Data ONTAP. Using this dashboard you can view or delete realms, or change the credentials for a realm. When you change the credentials for a realm, this change can affect a single machine or a group of ONTAP servers that all belong to the same realm.

The dashboard lists all of the realms defined within the app context for the ONTAP servers from which you collect API data. The page displays the defined realms, the user names associated with each realm, and the app to which it belongs.

Add Data Collection Node

Data collection nodes (DCN) are managed by the scheduler. In a search head clustering (SHC) deployment, the DCN scheduler must be deployed on its own, dedicated search head. Do not deploy the DCN Scheduler on any individual search heads within the SHC.

1. On the ONTAP Collection Configuration dashboard, in the Data collection node panel, select **Add Data Collection Node** to add a new data collection node to register it with your scheduler.
2. Configure this node to collect data from your environment by entering the settings for the data collection node. See the Data Collection Node configuration settings table below.

Field	Value
Splunk Forwarder URI	The address or port of the DCN. For example, https://<host_name_or_ip_address_of_DCN>:8089.
Splunk Forwarder Username	admin.
Splunk Forwarder Password	The administrator password. Make sure this password is not the Splunk Enterprise default admin password (changeme).
Worker Processes	Define the number of worker processes you want on the node. This is the number of processes you can run on the data collection node to process the data and forward it to the indexer(s). You can run a maximum of 8 processes per node at the default configuration. The number of worker processes must be one fewer than the number of CPU cores the vCenter Server system granted to the DCN. For example, if the DCN has four CPU cores, the number of worker processes is three.

3. Click **Save**.
4. Confirm that you correctly configured the DCN by verifying that the DCN, credential validation, and add-on validation all display a green check.
5. Repeat the steps for each DCN.

Add ONTAP Collection

Add one or more NetApp filers and configure them as the source of the data coming into Splunk. **Note**: Stop and restart the scheduler when you add or remove a filer from your environment.

To add a Filer:

1. On the **Collection Configuration** dashboard, in the ONTAP Collection Configuration panel, select **Add ONTAP Collection** to add a new NetApp filer.
2. Configure filer settings in the **Add ONTAP Collection** dialog.
    1. Enter the fully qualified domain name for the ONTAP server(s), for example, `test-na100.example.com`. This can be a comma delimited list of ONTAP servers.
    2. Use Realm based Credentials. Check this box if the credentials you are using to access your ONTAP server(s) are part of a realm (controlled by an authentication policy set for a defined set of users).
    3. Enter the Realm: Enter the name that defines the realm.
    4. Enter an ONTAP Username: Enter the username for the user of the app. For example, enter "administrator" as a local user, or enter "splunkadmin@splunk.local" as an Active Directory domain user. You may add an ONTAP User with a "Readonly" role assigned to the "ontapi" application or the "admin" user.
    5. Enter an ONTAP password. This is the password you use to access the the filer(s) in your NetApp environment.
    6. Collect All Performance Categories. This is enabled by default. All performance data is collected by the app unless you specifically request to only collect a subset of the data. To select specific performance data types, uncheck the box to disable automatic collection of all performance data. You can now select the performance categories you want to collect. Check the box beside each category of performance data (Volume, Disk, LUN, Aggregate, Vfiler, Qtree, Quota, System) you want to collect.
    7. Click **Save** to add a new ONTAP server and display it on the ONTAP Collection Configuration dashboard.
3. Validate that the ONTAP server is configured correctly. To validate that the ONTAP server is configured correctly the search head must be able to establish a connection to the filer. Validation can fail if the search head cannot directly connect to the filer. During the data collection process, all data is transferred through connections established by the data collection node (on the firewall ports 8089 and 8008). You configured the server correctly if it displays in the list of ONTAP servers in the ONTAP Collection Configuration panel and credential validation is valid and and connection validation is valid.

Step 3: Start the Scheduler

When your ONTAP servers are set up as data collection points and your data collection nodes are set up to gather API data, click **Start Scheduler**. The scheduler starts the data collection process and data is collected from the resources in your environment.

Note that if you add or modify credentials, restart the scheduler. This pushes the credentials out to the data collection nodes.

You have now completed all of the data collection configuration steps. Splunk is collecting ONTAP data from your environment and you can see the data when you look on the dashboards of the Splunk App for NetApp Data ONTAP.

Manage your ONTAP environment

Scheduler

The scheduling node (gateway) that runs the scheduler, typically on the search head, communicates with DCNs over port 8008 (default). If your environment uses port 8008 for another service, configure another port for communication between the DCN and the scheduling node. All data collection nodes do not have to communicate on the same port. You can configure the ports in the default stanza to implement the port change for all data collection nodes, or configure the port for each data collection node individually on a per stanza basis.

To set the port for the Hydra gateway, edit the configuration settings for the port on the scheduling node (usually implemented on the search head) in `$SPLUNK_HOME/etc/apps/Splunk_TA_ontap/local/hydra_node.conf`. See an example of the default setting for the app below.

```
[default]
gateway_port = 8008
```

The hydra gateway port, default value 8008, uses the SSL certs that Splunk Web uses. Splunk Enterprise generates these SSL certs by default, but you can override them in the `web.conf` file. The only information that travels machine-to-machine over the gateway port is hydra job assignment, configuration, and performance information. Hydra passes no credentials or session keys for the target environment though the gateway port. Credentials pass only through the storage/passwords endpoint on Splunkd on default port 8089.

You can add data collection nodes to the scheduler and configure worker processes on each during the installation of the app. Each time you access a node, the credentials for Splunk and the add-ons on that node are validated. Do this for each data collection node on an individual basis.

Check authentication and validation status of your ONTAP filers

In the Splunk Add-on for NetApp Data ONTAP connectivity and credential validation are checked for a filer, or for a set of filers, during the configuration of the app, only after you click **Save** in the **Edit ONTAP Collection** dialog or the **Add ONTAP Collection** dialog. If there is a change to your environment after you have installed the app and configured data collection, for example, if the password on a filer changes, that change is not automatically reflected in the **Collection Configuration** page. This change can prevent you from logging in to a filer and prevent data collection.

If you notice that you have stopped receiving data from a filer, go to the **Collection Configuration** page and click **Refresh Validation** to check if there are connectivity issues that the refresh action can identify for that filer.

After fixing the connectivity issues you can wait up to 30 minutes for the data to come in to the app as when a data collection node recognizes that it cannot connect to the filers, the worker processes limit that rate of attempts to login to the filer to once in a 30 minute period per filer.

You can also click Stop/Start scheduler to stop and restart data collection. This restarts data collection immediately from your ONTAP environment into Splunk.

Remember that if you add a new ONTAP filer as a target when the scheduler is running, you must stop and restart the scheduler to include the new filer as a data collection target. Refresh Validation does not update your Splunk environment.

Edit ONTAP Credentials

Delete a realm or change the credentials for a realm that you defined for a target asset (ONTAP server) or set of assets on the ONTAP Collection configuration dashboard.

Use caution when deleting credentials. The same credentials can be used by more than one consumer. When credentials are deleted and they are still used in other areas of your environment, then credential validation will fail for the consumers of those credentials.

Delete credentials that belong only to the Splunk Add-on for NetApp Data ONTAP, and only those that do not have an associated entry in the ONTAP Collection Configuration Page or an entry in the `ta_ontap_collection_config.conf` file.

To delete a realm

1. Select a realm from the table. The Edit ONTAP Credential dialog is displayed.
2. Click **Delete Server** to delete the credentials. This operation cannot be undone.
3. A confirmation dialog is displayed.
4. Click **Delete Server** to confirm your actions.

To change the credentials for a realm

1. Select a realm from the table. The Edit ONTAP Credential dialog is displayed.
2. Enter a new password in the Realm password text box.
3. Click **Save**.

Edit data collection node settings

To edit the configuration of your data collection node:

1. On the Collection Configuration dashboard, in the Data Collection Nodes panel, click on the node you want to modify.
2. You can edit the properties for the node, then click **Save** to update the configuration.

Delete a data collection node

Deleting a data collection node unregisters it from your scheduler. It no longer processes data or forwards data to your Splunk indexer.

To remove a data collection node from the scheduler configuration:

1. On the Collection Configuration dashboard, in the Data Collection Nodes panel, click on the node in the list, then click **Delete node**.
2. Confirm that you want to delete the node.
3. The node is removed from the list of nodes in the dashboard.

Edit ONTAP server settings

To edit filer settings:

1. On the Collection Configuration dashboard, in the ONTAP collection configuration panel, click on the filer you want to modify.
2. You can edit the properties for the filer, then click **Save** to update the configuration.

Delete a server

Deleting a server (filer) removes it from your Splunk environment. You will no longer collect data from this machine. When you add or remove a filer from your environment you must stop and restart the scheduler.

To delete a server:

1. On the Collection Configuration dashboard, in the ONTAP Collection Configuration panel, select the server from the list of target machines. The Edit ONTAP Collection dialog is displayed.
2. Click **Delete Server**.
3. Confirm that you want to delete the filer, then click **Save**.
4. The filer is removed as a data source and it is removed from the list of target machines in the dashboard.

Configure ONTAP servers

You can change the configuration settings of the ONTAP servers (7-mode or cluster mode) that you set up to work with the Splunk App for NetApp Data ONTAP. To do this, select the ONTAP server from the list of targets in the ONTAP Collection Configuration panel. The Edit ONTAP Collection dialog is displayed.

Configure performance category options

You can change the performance data collection options for your servers:

1. On the ONTAP Collection Configuration dashboard, in the ONTAP Collection Configuration panel, select the filer you want to reconfigure from the list of available filers. You can also use the ONTAP Server search box to find the specific filer.
2. To collect all performance data from the host, click "Collect All performance Categories".
3. To reduce the set of categories from which you want to collect performance data, uncheck the box. A list of performance categories is displayed (Volume, Disk, LUN, Aggregate, Vfiler, Qtree, Quota, System). Select the the check boxes that define the data set you want to collect.
4. Click **Save** to return to the dashboard.
5. To validate that you are only collecting data from the performance categories you selected, from the app menu, select **Settings**, then **App Data Volume**. The **App Data Volume** dashboard displays a list of data types and source types for the data you are collecting over the last 24 hour period.

Configure realm based access

You can set a server or group of servers to have realm based credentials. The ONTAP **Collection Configuration** page lists all of the realms defined within the app context.

1. In the **Add ONTAP Collection** dialog box, click **Use Realm based Credentials**.
2. Enter a realm.
3. Click **Save**.

Troubleshoot the Splunk Add-on for NetApp Data ONTAP

See the following troubleshooting tips if you're running into issues with the Splunk Add-on for NetApp Data ONTAP.

Troubleshoot your environment

To troubleshoot your environment, you can set the field `worker_log_level` in `hydra_node.conf` to reflect a new log level for a data collection node. The default log level for a data collection node is INFO. DEBUG will be the most verbose logging level.

1. On the search head that administers the Distributed Collection Scheduler, create a local version of `hydra_node.conf`
2. Edit `$SPLUNK_HOME/etc/apps/Splunk_TA_ontap/local/hydra_node.conf` to set the log level of for all data collection

nodes as per the following example:

```
[default]
â ¨gateway_port = 8008
â ¨capabilities = * â ¨
log_level = DEBUG
```

Distribute API requests across multiple data collection nodes

Distribute API requests across multiple data collection nodes (DCNs) to improve collection processing speed and to reduce collection fails. See the distribute API requests across multiple data collection nodes section of the *configure inputs* section of this manual.

Troubleshoot hydra scheduler and hydra worker error logs: `ValueError: unsupported pickle protocol: 3`

Problem

You receive the following error in the hydra worker logs:

```
 [ta_ontap_collection_worker://gamma:1361] Problem with hydra worker
ta_ontap_collection_worker://gamma:1361: unsupported pickle protocol: 3
Traceback (most recent call last):
  File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/hydra_worker.py", line 618, in run
    self.establishMetadata()
  File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/hydra_worker.py", line 64, in establishMetadata
    metadata_stanza = HydraMetadataStanza.from_name("metadata", self.app, "nobody")
  File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/models.py", line 610, in from_name
    host_path=host_path)
  File "/opt/splunk/lib/python2.7/site-packages/splunk/models/base.py", line 557, in get
    return self._from_entity(entity)
  File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/models.py", line 345, in _from_entity
    obj.from_entity(entity)
  File "/opt/splunk/lib/python2.7/site-packages/splunk/models/base.py", line 926, in from_entity
    super(SplunkAppObjModel, self).from_entity(entity)
  File "/opt/splunk/lib/python2.7/site-packages/splunk/models/base.py", line 684, in from_entity
    return self.set_entity_fields(entity)
  File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/models.py", line 544, in set_entity_fields
    from_api_val = wildcard_field.field_class.from_apidata(entity, entity_attr)
  File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/models.py", line 123, in from_apidata
    obj = cPickle.loads(b64decode(val))
ValueError: unsupported pickle protocol: 3
```

You receive the following error in the hydra scheduler logs:

```
ERROR [ta_ontap_collection_scheduler://nidhogg] [HydraWorkerNode] node=https://10.0.12.234:8089 is dead,
because some weird stuff happened: unsupported pickle protocol: 3
Traceback (most recent call last):
  File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/hydra_scheduler.py", line 1452, in setMetadata
    self.session_key)
  File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/models.py", line 610, in from_name
    host_path=host_path)
  File "/opt/splunk/lib/python2.7/site-packages/splunk/models/base.py", line 557, in get
    return self._from_entity(entity)
  File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/models.py", line 345, in _from_entity
    obj.from_entity(entity)
  File "/opt/splunk/lib/python2.7/site-packages/splunk/models/base.py", line 926, in from_entity
    super(SplunkAppObjModel, self).from_entity(entity)
  File "/opt/splunk/lib/python2.7/site-packages/splunk/models/base.py", line 684, in from_entity
    return self.set_entity_fields(entity)
  File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/models.py", line 544, in set_entity_fields
    from_api_val = wildcard_field.field_class.from_apidata(entity, entity_attr)
  File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/models.py", line 123, in from_apidata
    obj = cPickle.loads(b64decode(val))
ValueError: unsupported pickle protocol: 3
```

Cause

The add-on is unable to deserialize a Python object that's serialized with a Python version that's different than the version the add-on is running. For example, the add-on is unable to deserialize a Python object that's serialized by Pytho 3, but the add-on is running Python 2.

Resolution

1. From **Collection Configuration** page, stop the scheduler.
2. Stop Splunk on the DCN.
3. On the DCN, go to `$SPLUNK_HOME/etc/apps/Splunk_TA_ontap/local` and remove the hydra_metadata.conf file.
4. Start Splunk on the DCN.
5. Start Splunk on the **Collection Configuration** page.

Extracted Field Information

See the following fields not extracted for sourcetype="ontap:perf" and source="VolumePerfHandler" for ONTAP server v9.8 and v9.9.1:

- synchronous_frees
- synchronous_frees_rate
- asynchronous_frees_rate
- asynchronous_frees

Reference

Reference Tables

API reference

This is a list of the NetApp APIs used to get data from the NetApp Data ONTAP environment into Splunk.

Capability	7-mode	Cluster mode
aggr-get-iter		x
aggr-options-list-info		x
aggr-get-filer-info	x	x
aggr-get-root-name	x	
aggr-get-mediascrub-list-info	x	
aggr-space-list-info	x	
aggr-list-info	x	
aggr-options-list-info	x	
ems-message-get-iter		x
cifs-options-get-iter		x
cluster-identity-get		x
cluster-node-get-iter		x
export-rule-get-iter		x
disk-list-info	x	
export-policy-get-iter		x
lun-get-iter		x
lun-list-info	x	
nfs-exportfs-list-rules	x	
options-get-iter		x
options-list-info	x	
perf-object-counter-list-info	x	x
perf-object-list-info	x	x
perf-object-instance-list-info-iter		x
perf-object-get-instances		x
perf-object-get-instances-iter-start	x	
perf-object-get-instances-iter-next	x	
perf-object-get-instances-iter-end	x	

Capability	7-mode	Cluster mode
perf-object-instance-list-info	x	
qtree-list-iter-start	x	
qtree-list-iter-next	x	
qtree-list-iter-end	x	
qtree-list-iter		x
quota-list-entries-iter		x
quota-report-iter		x
quota-report-iter-start	x	
quota-report-iter-next	x	
quota-report-iter-end	x	
quota-status	x	
quota-status-iter		x
snapshot-list-info	x	
storage-disk-get-iter		x
system-api-list	x	x
system-get-info	x	
system-get-node-info-iter		x
system-get-ontapi-version	x	x
system-get-version	x	x
system-node-get-iter		x
vfiler-list-info	x	
vfiler-get-status	x	
volume-footprint-get-iter		x
volume-get-iter		x
volume-list-info-iter-start	x	
volume-list-info-iter-next	x	
volume-list-info-iter-end	x	
volume-scrub-list-info	x	
volume-mdeiascrub-list-info	x	
volume-options-list-info	x	
volume-space-get-iter		x
volume-storage-service-get-iter	x	
volume-move-get-iter		x
vserver-get-iter		x

Third Party Software

Credits

Some of the components included in Splunk App for NetApp Data ONTAP are licensed under free or open source licenses. We wi|-sh to thank the contributors to those projects.

View the license(s) associated with each component by selecting a component name on the left.

NM SDK

http://community.netapp.com/t5/Developer-Network-Articles-and-Resources/NetApp-Manageability-NM-SDK-Introduction-and-Dow

Version 5.2.2

Copyright Â© 2010 NetApp

Axios

https://github.com/axios/axios

Version 0.19.2

Copyright (c) 2014-present Matt Zabriskie

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files (the "Software"), to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included inall copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

Six

six.py version 1.12.0 Copyright (c) 2010-2020 Benjamin Peterson

Permission is hereby granted, free of charge, to any person obtaining a copy ofthis software and associated documentation files (the "Software"), to deal inthe Software without restriction, including without limitation the rights touse, copy, modify, merge, publish, distribute, sublicense, and/or sell copies ofthe Software, and to permit persons to whom the Software is furnished to do so,subject to the following conditions:

The above copyright notice and this permission notice shall be included in allcopies or substantial portions of the

ONTAP Collection Configuration Dashboard

The Data Collection Nodes panel

Look here for more details and explanation on adding, deleting, and editing data collection nodes.

Field	Description
Data collection node	This is a list of all nodes configured in your environment. The status of a node is always displayed. Look at the table to see that the node has passed all the validation checks. if validation fails, you will see an "invalid" status. The data collection node is identified in the table by it's Node management URI. Validation is enforced on the device management URI (as Splunk expects a certain protocol). Specify the full management URI of the Splunk installation. This is comprised of the protocol (https is required) , the address, and the port number for the management URI. For example, `https://testnode1:8089` Do this in the Add Data Collection Node dialog.
User	This is the Splunk Forwarder Username for the selected node. The default username is `admin`.
Worker processes	This is the number of processes you have running on the Data Collection Node to process the data and forward it to the Indexer(s). This is remote forwarder management. The minimum number of processes you can run in 1 and the maximum number is 8. Configure this when you create a new node or edit the settings of an existing node. Each time you access a node, the credentials for that node are validated.
Last updated	This date reflects the last time any updates were made to the data collection node.
Credential Validation	Credential validation is either valid or invalid. Valid indicates that credentials are established correctly.
Add Data Collection Node	Click **Add Data Collection Node** to add a new node.

Add/Edit Data Collection Node

To add a data collection node to your environment, click **Add Data Collection Node**. The Add Data Collection Node dialog is displayed. To make changes to a node that is already part of your environment, click on the node in the table. The Edit Data Collection node dialog is displayed.

Field	Description
Splunk Forwarder URI	This is the URI to the Splunk forwarder on your data collection node. Communication happens by default on port 8089. Enter the URI in the format `https://<ipaddress>:8089`
Splunk Forwarder Username	This is the forwarder username.
Splunk Forwarder password	This is the forwarder password.

Field	Description
Worker Processes	These are the worker processes that run on the node to do data collection tasks. They are managed directly by the scheduler. The maximum number you can have is 8 unless you do some advance configuration.
Cancel	Click **Cancel** to discontinue with your current operation.
Save	Click **Save** to save the details you entered for the data collection node. After saving the details the node appears in the table.
Delete node	This option is only available on the Edit Data Collection Node Dialog. Click **Delete node** to deleted the selected data collection node.

ONTAP Collection Configuration Panel

Look here for more details and explanation on adding, deleting, and editing ONTAP server settings.

Field	Description
Target	This is an ONTAP server configured in your environment. The ONTAP servers are identified in the table by their IP address.
User	This the user account for the ONTAP server. The default username is `admin`.
Credential validation	This can be valid or invalid. It is a report on the status of the credentials check. If the status is invalid, you have a problem accessing the ONTAP server, and you cannot collect data.
Connection Validation	This indicates the connection status to the ONTAP servers.
Realm	This is the name of the Realm to which the ONTAP servers belong.
Add ONTAP Collection	Add a new ONTAP server.
Refresh Validation	Click this button to get an updated status for any given filer. When you refresh, an attempt is made to connect with all of the connection targets and to validate the credentials for each target. Use "Refresh Validation" to explicitly check for connectivity to your ONTAP servers and to keep the status on the Collection Configuration page synchronized with the actual state of your environment.

Add/Edit ONTAP Collection

To add a new ONTAP server, click **Add ONTAP Collection**. To update the properties of an ONTAP server already configured in your environment, click on the server listed in the table. The Edit ONTAP Collection dialog is displayed.

Field	Description
ONTAP servers	This is the fully qualified domain name for the filer(s).
Use Realm Based Credentials	Select this box to add your server to a realm.
Realm	If you selected to use realm based credentials, then enter the name of the Realm.
ONTAP username	This is the username used to access the filer(s). The default is "admin".
ONTAP Password	This is the password for the filer(s).
Collect all performance categories	Click this check box to collect data from all sourcetypes. When unchecked, the list of categories for which the app collects performance data is listed. These categories are: Volume, Disk, LUN, Aggregate, Vfiler, Qtree, Quota, System.
Cancel	Click **Cancel** to discontinue with your current operation.
Save	

Field	Description
	Click **Save** to save the details you entered for the ONTAP server. After saving the details the ONTAP server is displayed in the list of targets in the ONTAP Collection Configuration table.

Stop Scheduler/ **Start Scheduler** - Click this button to start collecting data from your environment. Note that if you have the scheduler running and you want to add another ONTAP server to the Collection Configuration, you must stop the scheduler and restart it so that the new ONTAP server can be included.

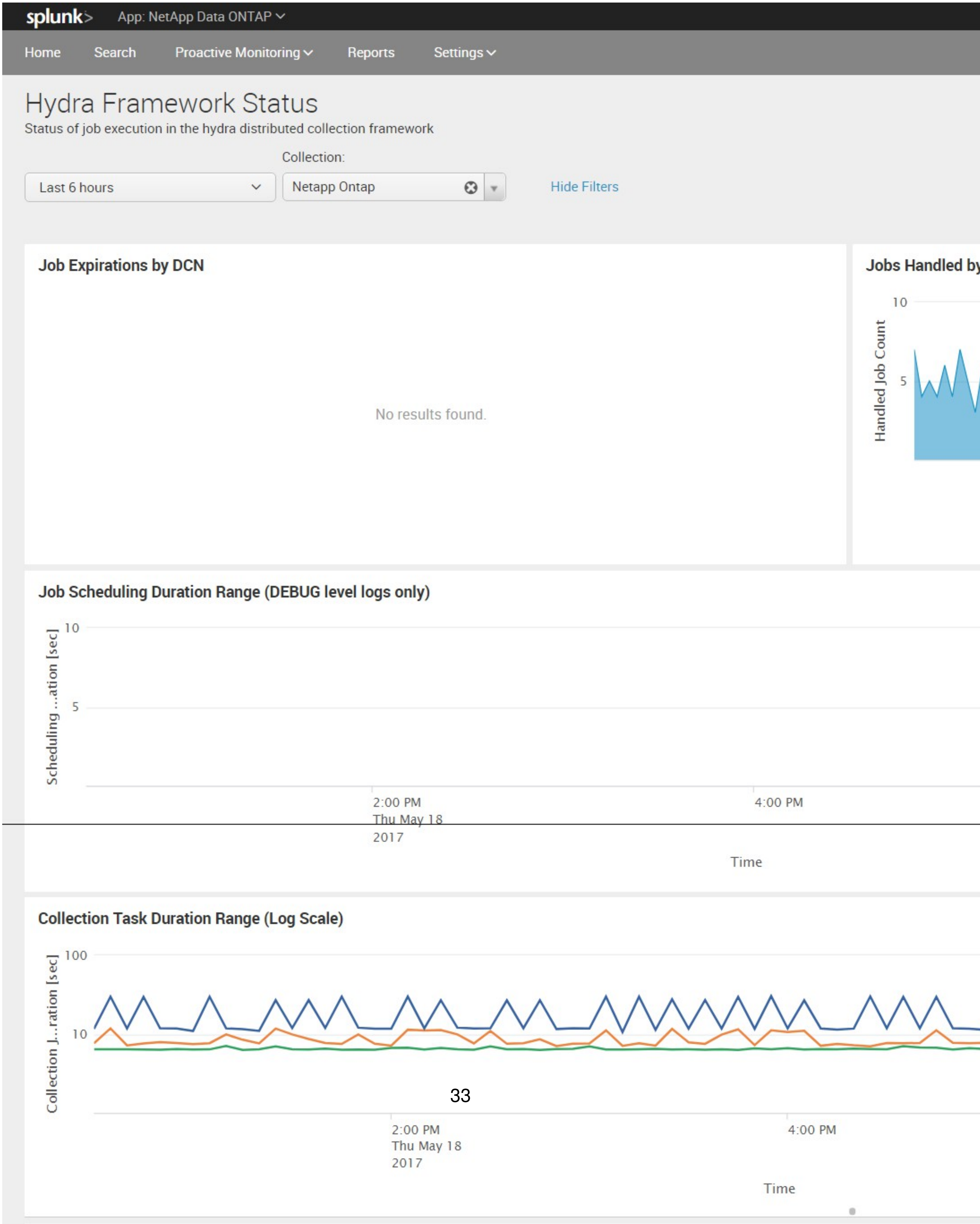
Hydra Framework Status

Use the Hydra Framework Status page to identify issues related to jobs handled by **SA-Hydra**. Page can be viewed by following the below link for your Splunk platform deployment.
`https://<SH>:8000/en-US/app/splunk_app_netapp/hydra_framework_status.`

Enable data population for this page.

1. Navigate to `Splunk_TA_ontap/local/input.conf`
2. Set the `log_level` to `DEBUG` for all enabled worker stanzas.
3. Save your changes and restart your Splunk platform deployment.

Dashboard name	Description
Job Expirations by DCN	Number of jobs assigned and expired on each DCN versus time. DCN (Worker) logs are required to populate this panel.
Jobs Handled by DCN	Number of jobs successfully completed by each DCN versus time. DCN (Worker) logs are required to populate this panel.
Job Scheduling Duration Range (DEBUG level logs only)	Average, Max and Min time taken for Scheduler to assign jobs to DCNs at every iteration versus time. It will populate when DEBUG level is enabled on your scheduler. Scheduler logs are required to populate this panel.
Collection Task Duration Range (Log Scale)	Minimum, Median and Maximum execution time to perform all the task. DCN (Worker) logs are required to populate this panel.
Median Task Performance Over Targets	Target (vCenter) and task wise median job execution time reported by Worker on DCN. DCN (Worker) logs are required to populate this panel.
Task Expiration Count Over DCN	Task wise no. of jobs assigned and expired on each DCN. DCN (Worker) logs are required to populate this panel.
Task Failure Count Over Target	Task wise no. of jobs assigned and failed on each DCN. DCN (Worker) logs are required to populate this panel.
Last 100 Worker Errors - excluding expiration	Last 100 errors occurred in worker processes in all DCNs excluding errors which occurred due to job expiration. DCN (Worker) logs are required to populate this panel.
Last 100 Scheduler Errors	Last 100 errors occurred in Scheduler process. Scheduler logs are required to populate this panel.



Hydra Framework Status

Status of job execution in the hydra distributed collection framework

Last 6 hours

Collection: Netapp Ontap

Job Expirations by DCN

No results found.

Jobs Handled by

Job Scheduling Duration Range (DEBUG level logs only)

Collection Task Duration Range (Log Scale)

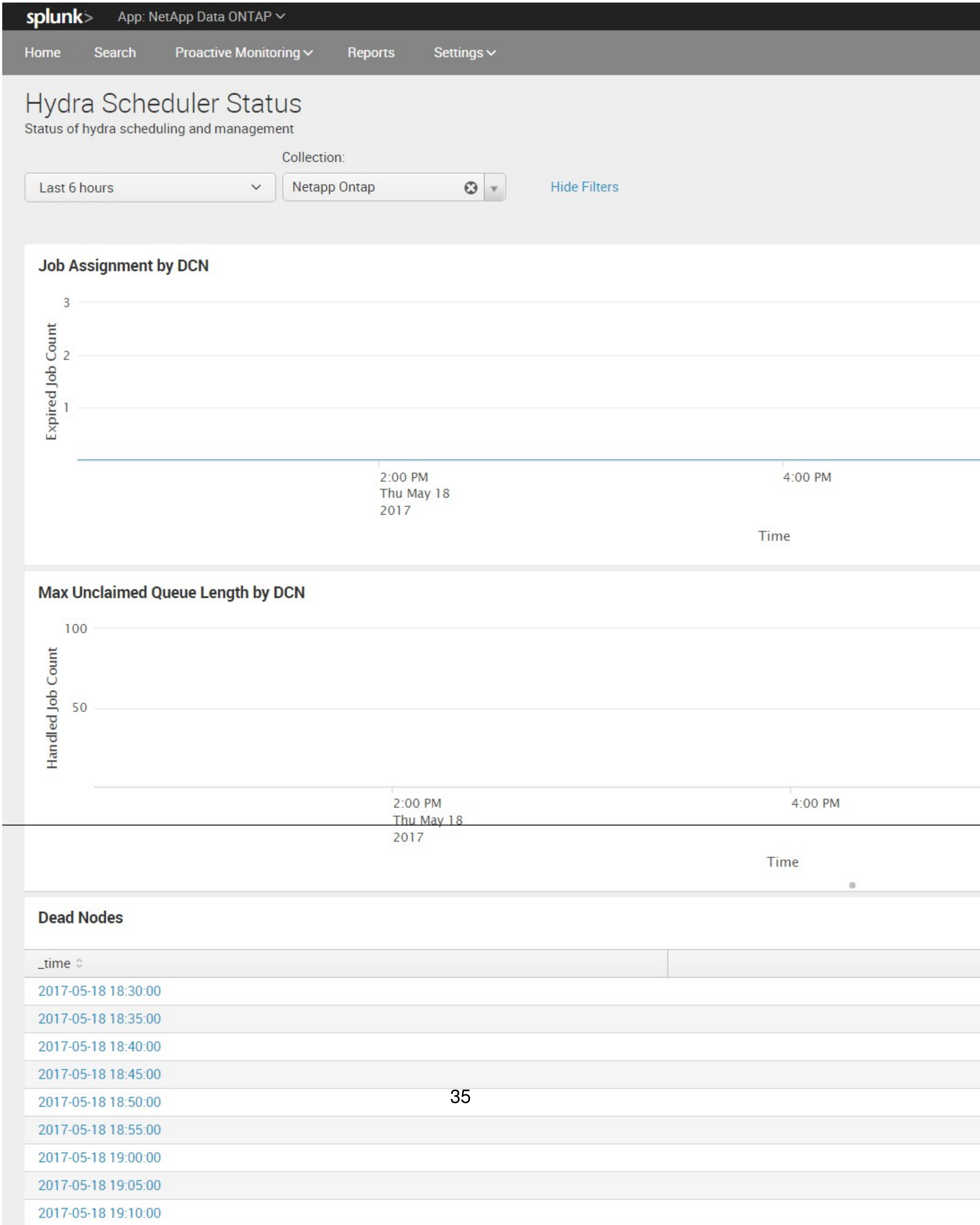
Hydra Scheduler Status

Use the Hydra Scheduler Status page to identify issues related to jobs handled your scheduler. Page can be viewed by following the below link for your Splunk platform deployment.
`https://<SH>:8000/en-US/app/splunk_app_netapp/hydra_scheduler_status`.

Enable data population for this page.

1. Navigate to `Splunk_TA_ontap/local/input.conf`
2. Set the `log_level` to `DEBUG` for all enabled worker stanzas.
3. Save your changes and restart your Splunk platform deployment.

Dashboard name	Description
Job Assignment by DCN	Number of jobs assigned to each DCN versus time. It will populate when DEBUG level is enabled on scheduler. Scheduler logs are required to populate this panel.
Max Unclaimed Queue Length by DCN	Number of unclaimed jobs reported by each DCN to Scheduler versus time. It will populate when DEBUG level is enabled on scheduler. Scheduler logs are required to populate this panel.
Dead Nodes	List of dead nodes (DCNs) and their count at every 5 minute interval. Scheduler logs are required to populate this panel.



Hydra Scheduler Status

Status of hydra scheduling and management

Last 6 hours

Collection: Netapp Ontap

Job Assignment by DCN

Max Unclaimed Queue Length by DCN

Dead Nodes

_time
2017-05-18 18:30:00
2017-05-18 18:35:00
2017-05-18 18:40:00
2017-05-18 18:45:00
2017-05-18 18:50:00
2017-05-18 18:55:00
2017-05-18 19:00:00
2017-05-18 19:05:00
2017-05-18 19:10:00

Upgrade the Add-On

Upgrade the Splunk Add-on for NetApp Data ONTAP to v3.0.1

Follow these steps when upgrading Splunk Add-on for NetApp Data ONTAP.

Step 1: Download the files from Splunkbase

Download the Splunk Add-on for NetApp Data ONTAP v3.0.1 from Splunkbase to a location in your environment.

Step 2: Upgrade the scheduler

Make sure splunk_ontap_admin role has admin_all_objects capability before upgrading the scheduler.

1. Navigate to the ONTAP **Collection Configuration** page of the Netapp add-on and click **Stop Scheduler**.
2. Stop Splunk on the scheduler instance.
3. Extract the contents of the Splunk Add-on for NetApp Data ONTAP to the `$SPLUNK_HOME/etc/apps` directory. This overwrites the previously installed add-on packages.
4. Go to `$PLUNK_HOME/etc/apps` and remove the following directories:
    1. SA-ONTAPIndex
    2. TA-ONTAP-FieldExtractions
    3. SA-VMNetAppUtils
5. If present, remove `/appserver` folder from SA-Hydra.
6. If present, remove the `/appserver/modules` folder from Splunk_TA_ontap.
7. Sync the `$SPLUNK_HOME/etc/apps/Splunk_TA_ontap/local /ta_ontap_collection.conf` by using saved search or without using saved search:

With saved search:

1. Restart the Splunk platform on the scheduler instance.
2. Go to **Settings>Searches, Reports, and Alerts**.
3. Select Splunk_TA_ontap from the dropdown of apps
4. Search for "Conf Synchronization" Saved search and click on "Run".
5. Check for the success message for all the stanzas of `ta_ontap_collection.conf`.

Without using saved search:

1. Navigate to `$SPLUNK_HOME/etc/apps/Splunk_TA_ontap/local /ta_ontap_collection.conf`. Find the property named `##"perf_whitelist"` in all the stanzas and replace it with `perf_includelist`.

Step 3: Upgrade the data collection node

1. Stop the Splunk on the DCN machine.
2. Extract the contents of the Splunk Add-on for NetApp Data ONTAP to `$SPLUNK_HOME/etc/apps` directory. This overwrites the previously installed add-on packages.
3. Go to `$PLUNK_HOME/etc/apps` and remove the following directories:
    1. SA-ONTAPIndex
    2. TA-ONTAP-FieldExtractions
    3. SA-VMNetAppUtils

4. If present, remove `/appserver` folder from SA-Hydra.
5. If present, remove the `/appserver/modules` folder from Splunk_TA_ontap.

(Optional) Step 4: Upgrade the indexer

1. Enable maintenance mode on the cluster master node.
2. Navigate to the `/apps` folder for your deployment. For a non-indexer cluster deployment, navigate to `$SPLUNK_HOME/etc/apps`. For the indexer clustering deployments, navigate to `SPLUNK_HOME/etc/master-apps`.
3. Overwrite SA-ONTAPIndex with the new version.
4. If you set up an indexer cluster, push the configuration bundle from the cluster master node.

Step 5: Upgrade the search head

1. Stop the Splunk on the machine.
2. Navigate to the `/apps` folder for your deployment. For non-search head cluster deployments, navigate to `$SPLUNK_HOME/etc/apps`. For search head clustering deployments, navigate to `$SPLUNK_HOME/etc/shcluster/apps/`.
3. Rename the package SA-VMNetAppUtils to "SA-VMNetAppUtils-backup".
4. Upgrade the add-on. This overwrites SA-Hydra and TA-ONTAP-FieldExtractions with the new version.
5. Go to `/apps/SA-VMNetAppUtils-backup/` and copy the local directory to the `/apps/SA-VMNetAppUtils/` directory.
6. Delete the SA-VMNetAppUtils-backup directory from `/apps`.
7. If present, remove the `/appserver` folder from SA-Hydra.
8. If you set up a search head cluster, push the app bundle from the deployer. The deployer restarts all the search head cluster members after the upgrade is applied. If the deployer does not restart the search head cluster members, perform a rolling restart.

Step 6: Start the scheduler

1. Start the Splunk on the DCN machine.
2. Start the Splunk on the scheduler machine.
3. Navigate to the ONTAP **Collection Configuration** page of the Netapp add-on.
4. Click **Start Scheduler** to start data collection.

Upgrade the Splunk Add-on for NetApp Data ONTAP from v3.0.1 to v3.0.2

Follow these steps when upgrading Splunk Add-on for NetApp Data ONTAP from v3.0.1 to 3.0.2.

Before you begin

These upgrade steps only apply to users upgrading from v3.0.1 to v3.0.2 of the Splunk Add-on for NetApp Data ONTAP. If you are using version previous to v3.0.1 (v2.1.91 or v3.0.0), follow the steps to upgrade to 3.0.1 to upgrade to v3.0.1 and then you can upgrade to v3.0.2 from v3.0.1 by following these steps.

Step 1: Upgrade the scheduler

Make sure the splunk_ontap_admin role has the admin_all_objects capability before upgrading the scheduler.

1. Go to the **ONTAP Collection Configuration** page of the Splunk Add-on for NetApp Data ONTAP and click **Stop Scheduler**.

2. Stop Splunk on the scheduler instance.
3. Download the Splunk Add-on for NetApp Data ONTAP v3.0.2 from Splunkbase and extract its contents to the $SPLUNK_HOME/etc/apps directory. This overwrites the Splunk_TA_ontap and SA-Hydra packages.

Step 2: Upgrade the data collection node

1. Stop Splunk on the data collection node machine.
2. Download the Splunk Add-on for NetApp Data ONTAP v3.0.2 from Splunkbase and extract its contents to the $SPLUNK_HOME/etc/apps directory. This overwrites the previously installed add-on packages.

Step 3: Upgrade the indexer

Enable maintenance mode on the cluster master node.

1. Download the Splunk Add-on for NetApp Data ONTAP Indexes v3.0.2 from Splunkbase and extract the SA-ONTAPIndex package to the /apps folder for your deployment.
    1. For a non-indexer cluster deployment, extract to $SPLUNK_HOME/etc/apps.
    2. For the indexer-clustering deployments, extract to $SPLUNK_HOME/etc/master-apps.
2. For indexer-clustering deployments, push the configuration bundle from the cluster master node.
3. Disable maintenance mode on the cluster master node.

Step 4: Upgrade the search head

1. Stop Splunk on the machine.
2. Download the Splunk Add-on for NetApp Data ONTAP Extractions v3.0.2 from Splunkbase and extract the TA-ONTAP-FieldExtractions package to the /apps directory for your deployment.
    1. For non-search head cluster deployments, extract to $SPLUNK_HOME/etc/apps.
    2. For search head clustering deployments, extract to $SPLUNK_HOME/etc/shcluster/apps/.
3. If you aren't using knowledge objects explicitly from the SA-VMNetAppUtils directory, remove the SA-VMNetAppUtils directory from the apps folder as the add-on doesn't use any KOs from this package. Keep the package as is, if you are using any of the knowledge objects from this package.
4. The Hydra troubleshooting dashboards (Hydra Framework Status and Hydra Scheduler Status) have been added to the TA-ONTAP-FieldExtractions package. So, you can remove the SA-Hydra directory from the Search head, if present.
5. For search head clustering deployments, push the app bundle from the deployer. The deployer restarts all the search head cluster members after the upgrade is applied. If the deployer doesn't restart the search head cluster members, perform a rolling restart.

Step 5: Start Splunk and the data collection node

1. Start Splunk on the data collection node machine.
2. Start Splunk on the scheduler machine.
3. Navigate to the **Collection Configuration** page of the Splunk Add-on for NetApp Data ONTAP on the scheduler tier.
4. Click **Start Scheduler** to start data collection.

Upgrade the Splunk Add-on for NetApp Data ONTAP from v3.0.1 to v3.0.3

See the following steps to upgrade the Splunk Add-on for NetApp Data ONTAP from v3.0.1 to 3.0.3:

1. Upgrade the scheduler.
2. Upgrade the data collection node.
3. Upgrade the indexer.
4. Upgrade the search head.
5. Start Splunk and the data collection node.

These upgrade steps only apply to users upgrading from v3.0.1 to v3.0.3 of the Splunk Add-on for NetApp Data ONTAP. If you are using a version previous to v3.0.1 (v2.1.91 or v3.0.0), upgrade to v3.0.1 to upgrade to v3.0.1 first. Then, you can upgrade to v3.0.3 from v3.0.1 by following these steps.

Upgrade the scheduler

1. Make sure the splunk_ontap_admin role has the admin_all_objects capability before upgrading the scheduler.
2. Go to the ONTAP Collection Configuration page of the Splunk Add-on for NetApp Data ONTAP and click Stop Scheduler.
3. Stop Splunk on the scheduler instance.
4. Download the Splunk Add-on for NetApp Data ONTAP v3.0.3 from Splunkbase and extract its contents to the `$SPLUNK_HOME/etc/apps` directory. This overwrites the Splunk_TA_ontap and SA-Hydra packages.

Upgrade the data collection node

1. Stop Splunk on the data collection node machine.
2. Download the Splunk Add-on for NetApp Data ONTAP v3.0.3 from Splunkbase and extract its contents to the `$SPLUNK_HOME/etc/apps` directory. This overwrites the previously installed add-on packages.

Upgrade the indexer

1. Enable maintenance mode on the cluster master node.
2. Download the Splunk Add-on for NetApp Data ONTAP Indexes v3.0.3 from Splunkbase and extract the SA-ONTAPIndex package to the /apps folder for your deployment.
    - For a non-indexer cluster deployment, extract to `$SPLUNK_HOME/etc/apps`.
    - For the indexer-clustering deployments, extract to `$SPLUNK_HOME/etc/master-apps`.
    - For indexer-clustering deployments, push the configuration bundle from the cluster master node.
3. Disable maintenance mode on the cluster master node.

Upgrade the search head

1. Stop Splunk on the machine.
2. Download the Splunk Add-on for NetApp Data ONTAP Extractions v3.0.3 from Splunkbase and extract the TA-ONTAP-FieldExtractions package to the /apps directory for your deployment.
    - For non-search head cluster deployments, extract to `$SPLUNK_HOME/etc/apps`.
    - For search head clustering deployments, extract to `$SPLUNK_HOME/etc/shcluster/apps/`.
3. If you aren't using knowledge objects explicitly from the SA-VMNetAppUtils directory, remove the SA-VMNetAppUtils directory from the apps folder as the add-on doesn't use any KOs from this package. Keep the package as is, if you are using any of the knowledge objects from this package.
4. The Hydra troubleshooting dashboards (Hydra Framework Status and Hydra Scheduler Status) have been added to the TA-ONTAP-FieldExtractions package. So, you can remove the SA-Hydra directory from the Search head, if present.
5. For search head clustering deployments, push the app bundle from the deployer. The deployer restarts all the search head cluster members after the upgrade is applied. If the deployer doesn't restart the search head cluster

members, perform a rolling restart.

Start Splunk and the data collection node

1. Start Splunk on the data collection node machine.
2. Start Splunk on the scheduler machine.
3. Navigate to the Collection Configuration page of the Splunk Add-on for NetApp Data ONTAP on the scheduler tier.
4. Click Start Scheduler to start data collection.

Troubleshooting

Troubleshoot the Splunk Add-on for NetApp Data ONTAP

See the following troubleshooting tips if you're running into issues with the Splunk Add-on for NetApp Data ONTAP.

Troubleshoot your environment

To troubleshoot your environment, you can set the field `worker_log_level` in `hydra_node.conf` to reflect a new log level for a data collection node. The default log level for a data collection node is INFO. DEBUG will be the most verbose logging level.

1. On the search head that administers the Distributed Collection Scheduler, create a local version of `hydra_node.conf`
2. Edit `$SPLUNK_HOME/etc/apps/Splunk_TA_ontap/local/hydra_node.conf` to set the log level of for all data collection nodes as per the following example:

```
[default]
â ¨gateway_port = 8008
â ¨capabilities = * â ¨
log_level = DEBUG
```

Distribute API requests across multiple data collection nodes

Distribute API requests across multiple data collection nodes (DCNs) to improve collection processing speed and to reduce collection fails. See the distribute API requests across multiple data collection nodes section of the *configure inputs* section of this manual.

Troubleshoot hydra scheduler and hydra worker error logs: `ValueError: unsupported pickle protocol: 3`

Problem

You receive the following error in the hydra worker logs:

```
 [ta_ontap_collection_worker://gamma:1361] Problem with hydra worker
ta_ontap_collection_worker://gamma:1361: unsupported pickle protocol: 3
Traceback (most recent call last):
  File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/hydra_worker.py", line 618, in run
    self.establishMetadata()
  File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/hydra_worker.py", line 64, in establishMetadata
    metadata_stanza = HydraMetadataStanza.from_name("metadata", self.app, "nobody")
  File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/models.py", line 610, in from_name
    host_path=host_path)
  File "/opt/splunk/lib/python2.7/site-packages/splunk/models/base.py", line 557, in get
    return self._from_entity(entity)
  File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/models.py", line 345, in _from_entity
    obj.from_entity(entity)
  File "/opt/splunk/lib/python2.7/site-packages/splunk/models/base.py", line 926, in from_entity
    super(SplunkAppObjModel, self).from_entity(entity)
  File "/opt/splunk/lib/python2.7/site-packages/splunk/models/base.py", line 684, in from_entity
    return self.set_entity_fields(entity)
  File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/models.py", line 544, in set_entity_fields
    from_api_val = wildcard_field.field_class.from_apidata(entity, entity_attr)
  File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/models.py", line 123, in from_apidata
    obj = cPickle.loads(b64decode(val))
ValueError: unsupported pickle protocol: 3
```

You receive the following error in the hydra scheduler logs:

```
ERROR [ta_ontap_collection_scheduler://nidhogg] [HydraWorkerNode] node=https://10.0.12.234:8089 is dead,
because some weird stuff happened: unsupported pickle protocol: 3
Traceback (most recent call last):
  File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/hydra_scheduler.py", line 1452, in setMetadata
    self.session_key)
  File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/models.py", line 610, in from_name
    host_path=host_path)
  File "/opt/splunk/lib/python2.7/site-packages/splunk/models/base.py", line 557, in get
    return self._from_entity(entity)
  File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/models.py", line 345, in _from_entity
    obj.from_entity(entity)
  File "/opt/splunk/lib/python2.7/site-packages/splunk/models/base.py", line 926, in from_entity
    super(SplunkAppObjModel, self).from_entity(entity)
  File "/opt/splunk/lib/python2.7/site-packages/splunk/models/base.py", line 684, in from_entity
    return self.set_entity_fields(entity)
  File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/models.py", line 544, in set_entity_fields
    from_api_val = wildcard_field.field_class.from_apidata(entity, entity_attr)
  File "/opt/splunk/etc/apps/SA-Hydra/bin/hydra/models.py", line 123, in from_apidata
    obj = cPickle.loads(b64decode(val))
ValueError: unsupported pickle protocol: 3
```

Cause

The add-on is unable to deserialize a Python object that's serialized with a Python version that's different than the version the add-on is running. For example, the add-on is unable to deserialize a Python object that's serialized by Pytho 3, but the add-on is running Python 2.

Resolution

1. From **Collection Configuration** page, stop the scheduler.
2. Stop Splunk on the DCN.
3. On the DCN, go to `$SPLUNK_HOME/etc/apps/Splunk_TA_ontap/local` and remove the hydra_metadata.conf file.
4. Start Splunk on the DCN.
5. Start Splunk on the **Collection Configuration** page.