Dell ECS App for Splunk Enterprise

Configuration and Deployment

June 2022

H18011.3

White Paper

Abstract

This document describes how to deploy and configure the Dell ECS Technology Add-on and App for Splunk Enterprise.

Dell Technologies

Copyright

Published in the USA June 2022 H18011.3.

Contents

Executive summary

Overview

The Splunk App for Dell ECS enables a Splunk Enterprise administrator to view performance information and detailed metrics from ECS Virtual Data Center (VDC) through the ECS Technical Add-on (TA). It also enables them to present the metrics in prebuilt dashboards, tables, and time charts for analysis and drill-down views with detailed operational information.

Download the Dell ECS App for Splunk from Splunkbase here.

Download the Dell ECS Add-on for Splunk from Splunkbase here.

Audience

This document is intended for administrators who deploy and configure Splunk Applications.

Revisions

Date	Description
October 2019	Initial release
December 2019	Updated prerequisite information
March 2022	Updated template, supported versions, and general notes
June 2022	Content update

We value your feedback

Dell Technologies and the authors of this document welcome your feedback on this document. Contact the Dell Technologies team by email.

Author: Rich Paulson

Note: For links to other documentation for this topic, see the ECS Info Hub.

Solution overview

Solution architecture

The application consists of two elements:

- The Add-on runs collector scripts to gather metrics from the ECS nodes. Then, it stores this data in a Splunk index which the ECS App for Splunk uses to build the dashboards. Syslog and access logs are also forwarded to the Splunk Heavy Forwarder to be indexed and to populate various dashboards.
- The main application parses the indexed data that was collected from the ECS Add-on app and runs searches on the indexed data to populate the various dashboards.

The following high-level architecture diagram shows a distributed Splunk environment where ECS data is collected by a heavy forwarder, sent to an indexer, and displayed by the application which resides on a search head.

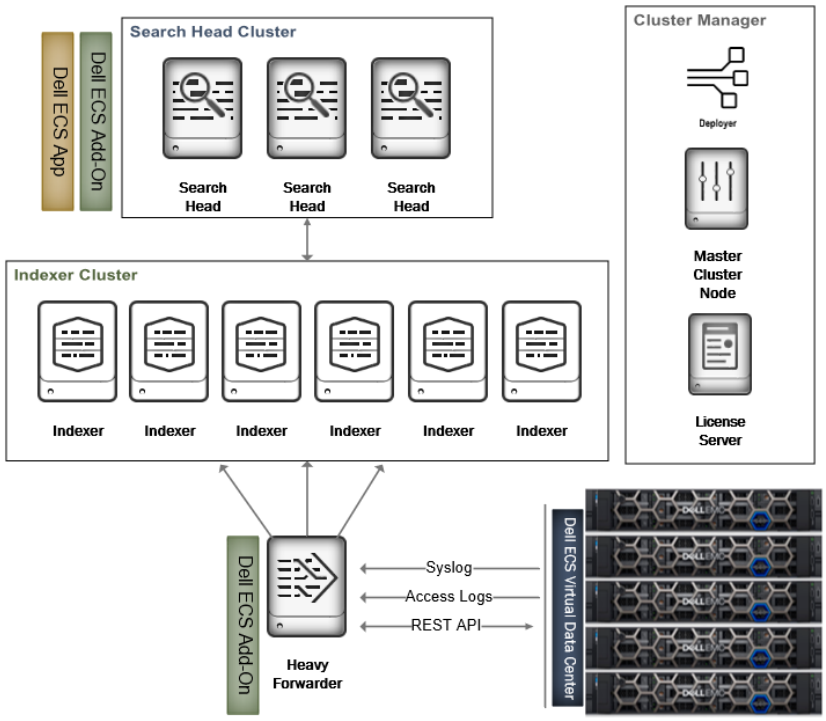


Figure 1. High-level architectural diagram

Solution requirements

You must meet the following requirements before installing the Technology Add-on (TA) and App.

Table 1. Requirements

Requirement	Description
ECS	Release 3.3.x and later
Splunk Enterprise	Version 8.1 and later

Dashboards

The ECS App for Splunk Enterprise includes several dashboards that present data collected from ECS. The following table illustrates the reporting levels and submenus.

Table 2. Reporting levels

Reporting level	Dashboards
Overview	ECS VDC Health and Status
Monitor	Metering and Disk bandwidth
Events	Syslog and Audit events
Alerts	VDC Alerts
Capacity Utilization	VDC Capacity, Garbage Collection, Erasure Coding, CAS processing and Ingest over Time
Transactions	Transaction Requests and Performance
Geo Replication	Rates and Chunks, RPO, Failover, and Bootstrap processing
Data Access Log	Several submenu dashboards that display S3 data access metrics
CAS Logs Analysis	Several submenu dashboards that display CAS data access metrics

Prerequisites

Note the following prerequisites before installing the Splunk App for ECS.

Port Access: This app uses the ECS Management API which communicates on port 4443. This port must be opened for the Add-on to collect metrics from the ECS VDC.

Data Access Logs:

- For ECS 3.4 and earlier versions, an RPQ must be requested to configure data access forwarding on the ECS VDCs. Contact your local account teams to submit the RPQ.
- ECS 3.5 and later versions allow for easy configuration to export data access logs to an external SYSLOG target, without requiring an RPQ. This forwarding configuration is a requirement for enabling or using the ECS Splunk App.
- See the knowledge base article ECS How to Export ECS access logs to external SYSLOG target for instructions.

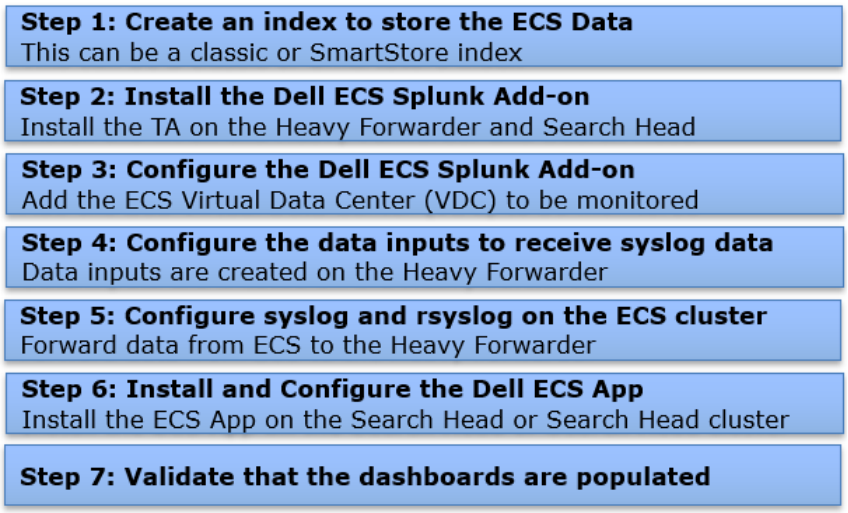
ECS Management User: We recommend creating a Management User from the ECS Web Portal with read-only (system monitor) privileges.

Solution implementation

Implementation workflow

This section describes the general steps to deploy the Splunk App and Technology Add-on for ECS. The following steps assume a heavy forwarder is being used, however, data access logs can also be forwarded directly to the indexers.

The following workflow shows the steps detailed in Installation and configuration steps.



Installation and configuration steps

Create an index to store ECS data

An existing Splunk index can be used to store the incoming data from ECS. However, we recommend creating a new one. The index can be a SmartStore or Non-SmartStore index.

Note: If using a Heavy Forwarder, you must create the same index name on it.

See this document to create a SmartStore index with ECS.

Install the Dell ECS Splunk Technology Add-on

The TA is installed on both the **Heavy Forwarder** and **Search Head**. It can be installed through the UI or by unpacking it from the CLI.

Install from the UI

1. Log in to Splunk Web, and go to **Apps** > **Manage Apps**.
2. Click **install app from file.**
3. Click **Choose file**, and select the Dell ECS Add-on installation file.
4. Click **Upload**.
5. Restart Splunk.

Install from the CLI

1. Transfer the TA package to the Heavy Forwarder and Search Head.
2. SSH to the server.
3. Use the following command to unpack the file:

```
tar xvzf <name of ECS TA package> -C /$SPLUNK_HOME/etc/apps/
```

4. Restart Splunk.

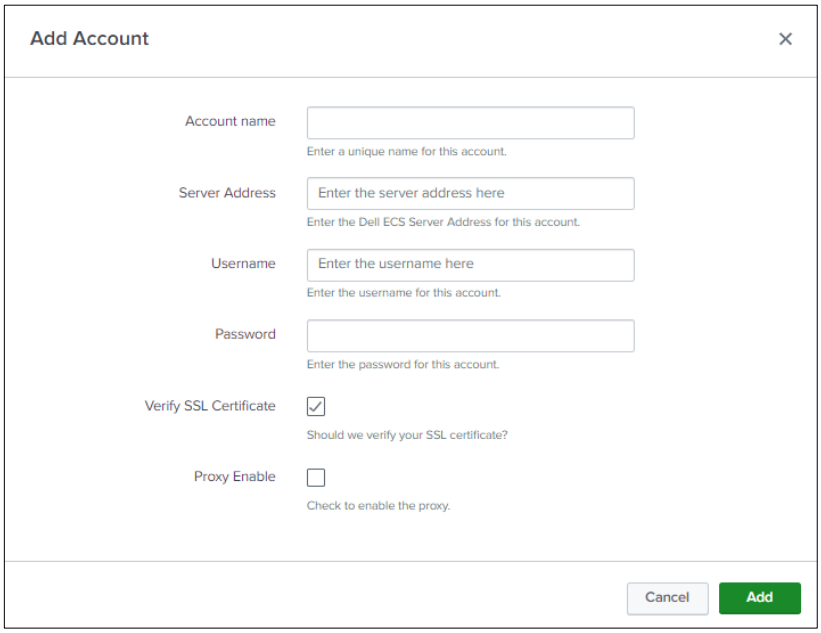
Configure the Dell ECS Splunk Technology Add-on

When Splunk has restarted, log in to the Heavy Forwarder UI to configure the Add-on.

Note: Configuration of the TA is only performed on the Heavy Forwarder or indexer. No configuration is necessary on the Search Head.

Configuration tab

1. Click the **Configuration** tab next to the **Inputs** tab.
2. Click the **Add** button to add the information for an ECS VDC.



Account Name: Enter a unique name for the ECS VDC.

Server Address: Enter the IP of one of the ECS Nodes. **Do not use a Virtual IP.**

Username: Enter the ECS Management user. An existing user can be used, or a new one can be created specifically for the Splunk App for ECS.

Password: Enter the password for the ECS Management User.

Verify SSL Certificate: Verify the ECS management API SSL certificate.

Proxy Enable: Details for the proxy (host, port) must be entered if the checkbox is enabled.

Note: If Verify SSL Certificate is enabled, you must append the certificate to the **$SPLUNK_HOME/etc/apps/TA-dellecs/ta_dell_ecs/requests/cacert.pem** file. For safety purposes, take a backup of cacert.pem before appending the SSL certificate.

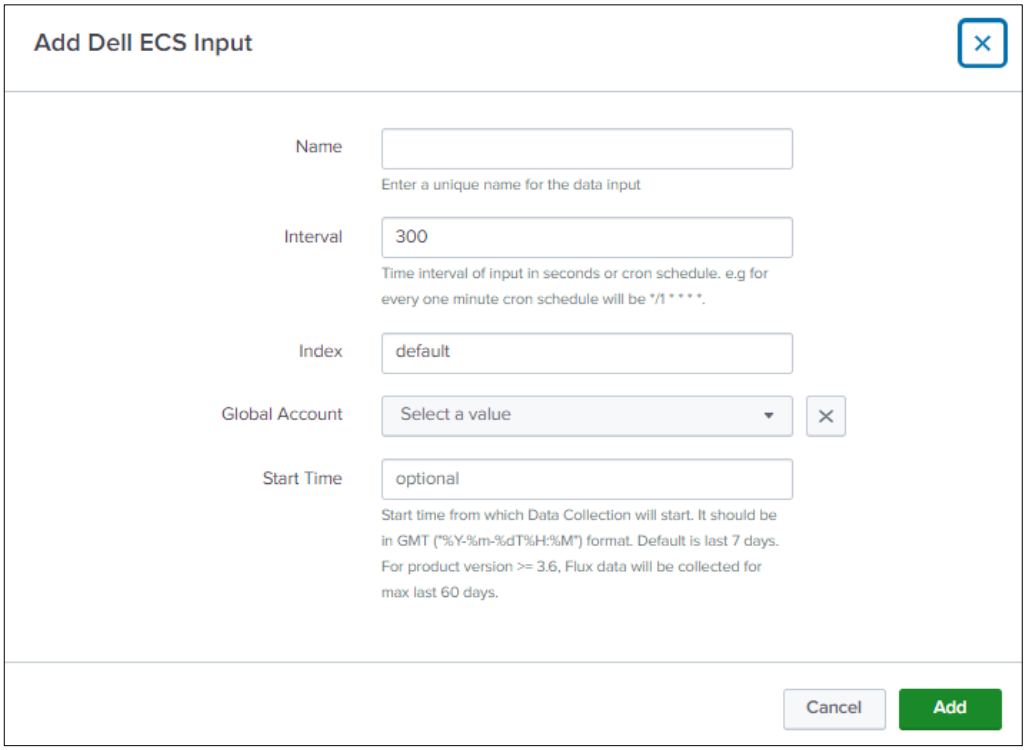
Create an account for each ECS VDC.

Inputs tab

1. Click the **Create New Input** button from the **Inputs** tab.
2. Multiple inputs are required for each ECS VDC.
   - **Dell ECS Input** indexes all the data into the Splunk except Namespace and Bucket data.
   - **Dell ECS Namespace Input** indexes Namespace data only.
   - **Dell ECS Buckets Input** indexes Buckets data only.

   Note: If multiple inputs are created using the same global account, there will be duplicate events in the Splunk index.

   The individual inputs control how often to collect information from ECS. For instance, if there are several namespaces, you can set the interval in the Dell ECS Namespace Input to once per day to limit the number of API calls that are performed.
3. Create each input for each ECS VDC.



Name: Enter a unique name for the Input (VDC1, VDC1_Namespace, VDC1_Buckets).

Interval: Keep the default or enter a new interval.

Index: Select the index to store the ECS data (use the index created in Create an index to store ECS data).

Global Account: This should correspond to the VDC that is created in the Configuration tab.

Start Time: (Optional) Specify when Data Collection should start.

Start Time: (Optional) Specify when Data Collection should start.

Note: For ECS version 3.6 and later, the maximum number of days of historical data that can be collected is 60.

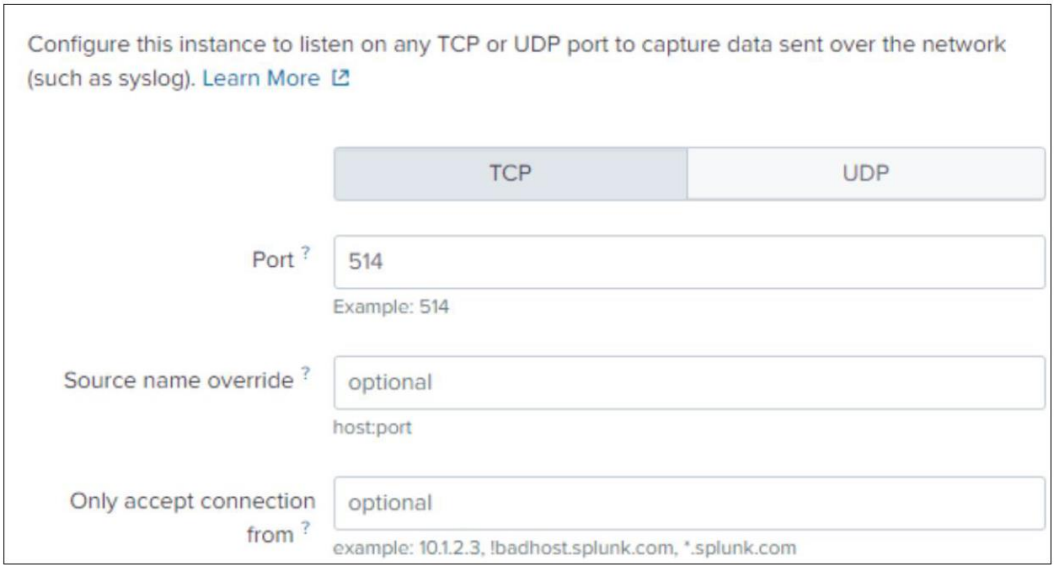
Configure data inputs to receive syslog and access data from the ECS VDCs

Create Data Inputs on the Heavy Forwarder to receive syslog and data access logs from ECS.

Syslog Forwarding

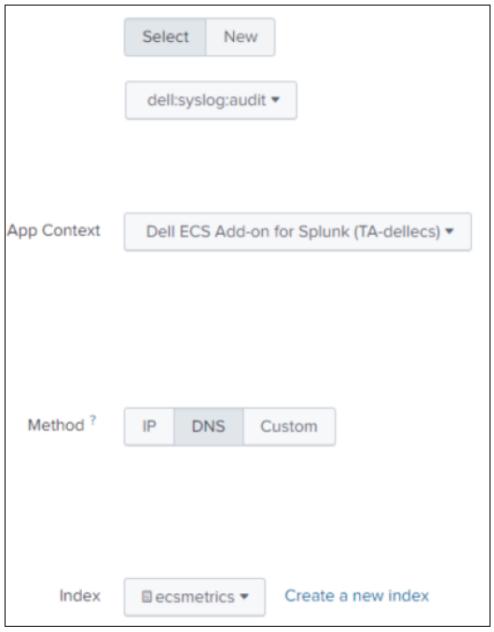
The following example configures a Data Input to receive syslog data from ECS to the Heavy Forwarder using the TCP protocol.

1. Click **TCP** from the **Data Inputs** menu.
2. Click the **New Local TCP** button at the top-right corner of the page.
3. Enter the port on which the forwarder will be listening and optionally override the source name (default will be tcp:<port>) and connections to accept. Click **Next**.



4. Click **Next**.

5. For **Source Type** click **Select** and choose **Custom>dell:syslog:audit**.
   a. **App Context:** Dell ECS Add-on for Splunk (TA-Dellecs).
   b. **Method:** Choose the host value to display in searches.
   c. **Index**: Choose the index. This should be the same index the collector is using to store ECS data.

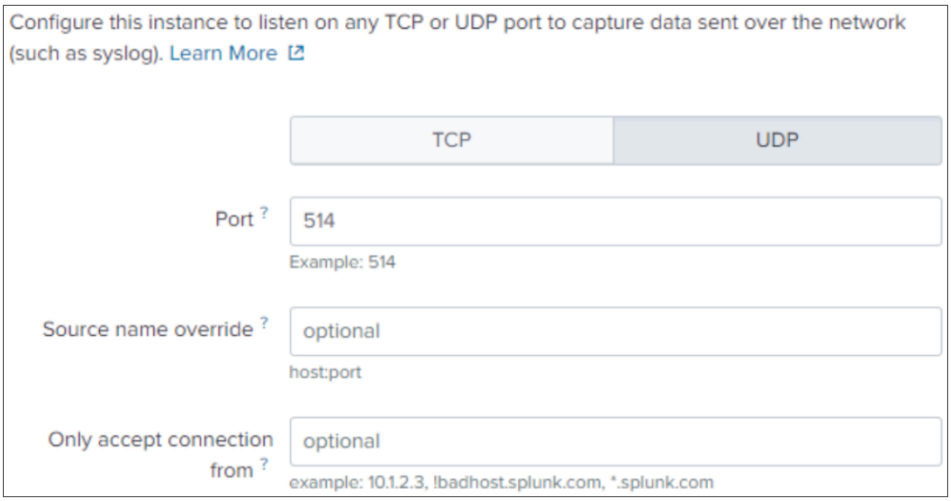


6. Click the **Review** button to review the setup, and click **Submit**.

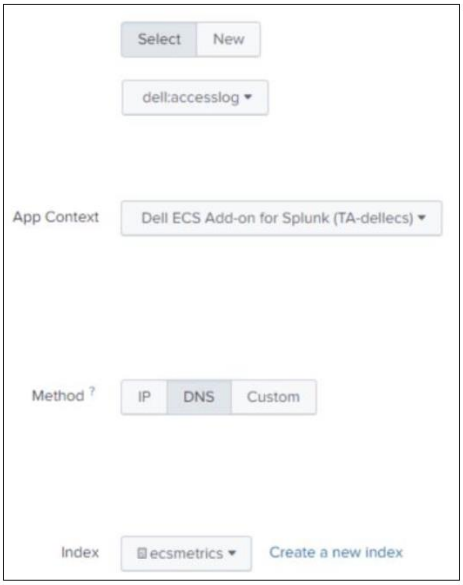
Access Log Forwarding

The following example configures a Data Input to receive access logs from ECS to the Heavy Forwarder using the UDP protocol.

1. Click **UDP** from the **Data Inputs** menu.
2. Click the **New Local UDP** button at the top-right corner of the page.
3. Enter the port on which the forwarder will be listening, and optionally override the source name (default will be udp:<port>) and connections to accept. Click **Next.**



4. For **Source Type**, click **Select**, and choose **Custom>dell:accesslog**.
   a. **App Context:** Dell ECS Add-on for Splunk (TA-Dellecs).
   b. **Method:** Choose the host value to display in searches.
   c. **Index:** Choose the index. This should be the same index the TA is using to store ECS data.

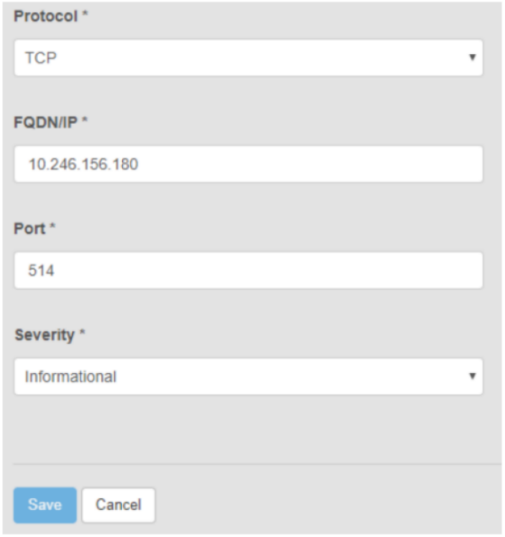


5. Click the **Review** button to review the setup, and click **Submit**'

Configure syslog and rsyslog on the ECS VDCs

Configure ECS to forward syslogs to the Heavy Forwarder

1. Log in to the ECS Web Portal, and go to **Settings** > **Event Notifications** > **Syslog**.
    a. Click the **New Server** button.
    b. Select the Protocol (must match the protocol defined in the Splunk Data input that was previously created).
    c. Enter the FQDN or IP of the Heavy Forwarder.
    d. Enter the port number to forward data to (must match the port number defined in the Splunk Data Input that was previously created).
    e. Enter the severity.



2. Click **Save**.

Configure ECS to forward Data Access logs to the Heavy Forwarder

---

Note: For ECS 3.4 and earlier, you must request an RPQ to configure data access forwarding on the ECS VDC. Contact your local account team to submit the RPQ.

Forwarding of the data access logs can be self-configured when using ECS 3.5 and **later. See** the **k**nowledge base **a**rticle ECS How to Export ECS access logs to external SYSLOG target for instructions.

The Port and Protocol must match the Data Input which was created to receive data access logs. The Target is the IP or FQDN of the Heavy Forwarder or indexers.

Note: These changes may not persist after operating system upgrades. It is advised that the settings are verified after an upgrade.

Install and configure the Dell ECS App for Splunk

The App is installed on the **Search Head**. It can be installed through the UI or by unpacking it from the CLI.

Install from the UI

1. Log in to Splunk Web, and go to **Apps** > **Manage Apps**.
2. Click **install app from file.**
3. Click **Choose file**, and select the Dell ECS App installation file.
4. Click **Upload**.
5. Restart Splunk.

Install from the CLI

1. Transfer the App package to the Search Head.
2. SSH to the server.
3. Use the following command to unpack the file:

   ```
   tar xvzf <name of ECS App Package> -C /$SPLUNK_HOME/etc/apps/
   ```

4. Restart Splunk.

Configure the Base value

1. Go to **Apps** > **Manage Apps**.
2. Select the filter for **Dell ECS App for Splunk**, and click **Actions** > **Set up**.
3. Set up the base value, and click **Save**.

For example, If the base value is 2, 1024 bytes will be converted to 1 KiB. If the base value is 10, 1000 Bytes will be converted to 1 KB.

Configure the index name for the Macro

1. Go to **Settings** > **Advanced search** > **Search macros**.
2. Select the filter for **Dell_ECS_index,** and click **Dell_ECS_index** under the name.
3. Edit the macro definition **(index = <index name>).**

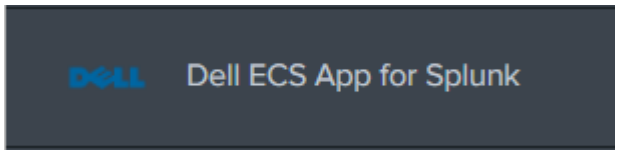
   Note: This index should be the same index that was created in Create an index to store ECS data and used to configure the Technology Add-on.

4. Click **Save**.

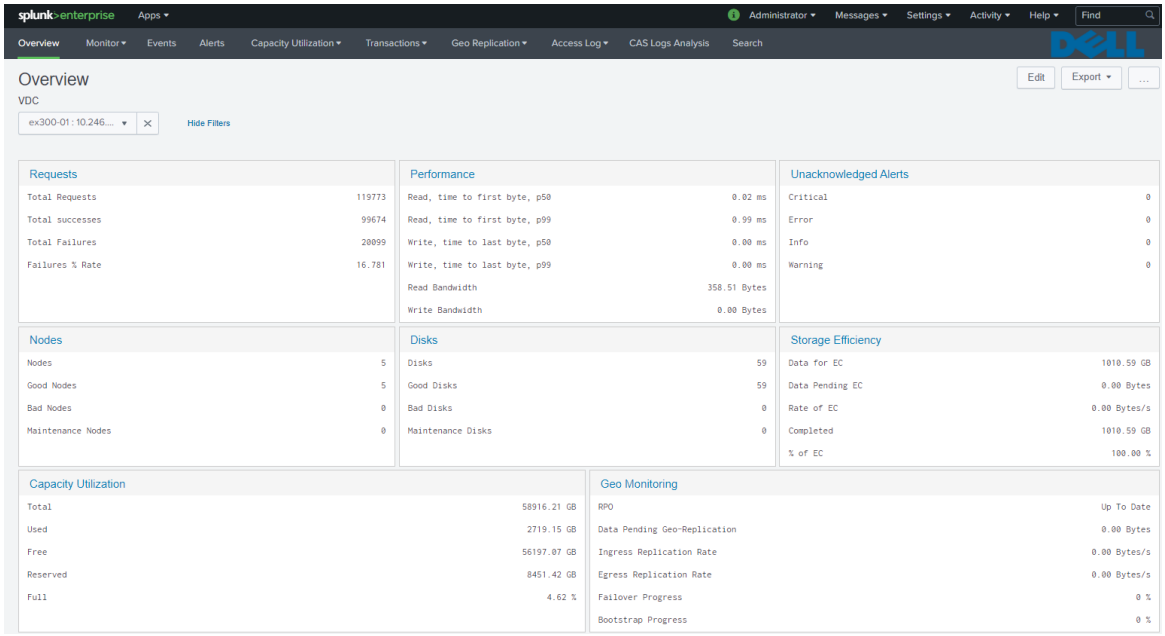
Validate that data is getting collected

To view the data that is logged by the Dell ECS Add-on for Splunk, click the **Search** tab, and search for the **Dell_ECS_index** macro.

Go to the Splunk App for ECS on the Splunk Search Head where the app was installed, and click the application.



Verify that each VDC that was configured is displayed in the **VDC** drop-down menu.



Note: Because Data Collection for the overview page looks back 24 hours, data may not be displayed immediately.

If dashboards are not populated, go to the search field, go to **Settings** > **Searches, Reports, and Alerts**, and run the **dell_vdc_list** saved search.

Appendix: Notes

The following table contains general notes and advisements.

Description	Detail
Monitor > Disk Bandwidth data collection methodology	ECS data is collected by using a one-hour sliding window to reduce the impact of data collection on the ECS cluster. This means that the Monitor > Disk Bandwidth panel may not show complete data depending on the date/time range that was selected.
Transactions>Performance panel	This panel is similarly to the above panel. This panel may show a delay in data of up to five minutes due to the frequency period this data is collected.
Do not use a VIP when configuring the account details	The use of a VIP when configuring the account in the Technical Add-on will result in the Performance data to not be displayed in ECS version 3.6 and later. An IP of one of the nodes in the VDC should be used.
A ReadTimeoutError may occur on VDCs which contain many nodes. The timeout can be modified by following these steps. **Note:** The higher the value, the higher amount of time the client will wait until a timeout occurs (in seconds).	Disable the Inputs. Go to the location: **$SPLUNK_HOME/etc/apps/TA-dellecs/bin,** and make the below change: • Copy **ecs_connect.py** and rename it to **ecs_connect.py.bak** to create a backup. • In **ecs_connect.py,** find the string: **self.TIMEOUT=15.** • Change the value of timeout from 15 to 60 (60 seconds). • **Note:** This change will affect all three modular inputs (login and data collection).

Appendix: Technical support and resources

Dell Technologies documentation

The following Dell Technologies documentation provides other information related to this document. Access to these documents depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.

- ObjectScale and ECS Info Hub
- Support: Contact dell-support@crestdatasys.com