Configuration and Deployment

Dell EMC ECS App for Splunk Enterprise Configuration Guide

Abstract

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

December 2019

H18011.1

Revisions

Date	Description
October 2019	Initial release
December 2019	Updated prerequisite information

Acknowledgements

This paper was produced by the Unstructured Technical Marketing Engineering and Solution Architects team.

Author: Rich Paulson

Table of contents

Executive summary

The Splunk App for Dell EMC ECS allows a Splunk® Enterprise administrator to view performance information, and detailed metrics from ECS VDCs through the ECS Technical Add-on (TA) and present them in pre-built dashboards, tables and time charts for in-depth analysis and drill-downs.

Download the Dell EMC ECS App for Splunk from Splunkbase here

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

Objectives

The objectives of the guide are to provide the steps to deploy and configure the Splunk Technology Add-on (TA) and Splunk Application for ECS.

Audience

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

1 Solution overview

This section provides an overview of the Dell EMC ECS App for Splunk Enterprise.

1.1 Solution architecture

The application consists of two elements which are installed on a Splunk Search Head and Heavy Forwarder.

- The Add-on runs collector scripts that utilize the ECS Management API to gather metrics from the ECS nodes. It stores this data in a Splunk index which the Dell EMC ECS App for Splunk uses to build the dashboards. Syslog and access logs are also forwarded to the Splunk Heavy Forwarder and indexed to populate various dashboards.
- The main application receives indexed data from the Dell EMC ECS Add-on app and runs searches on the indexed data to build the various dashboards.

The below high-level architecture diagram illustrates where the elements are installed.

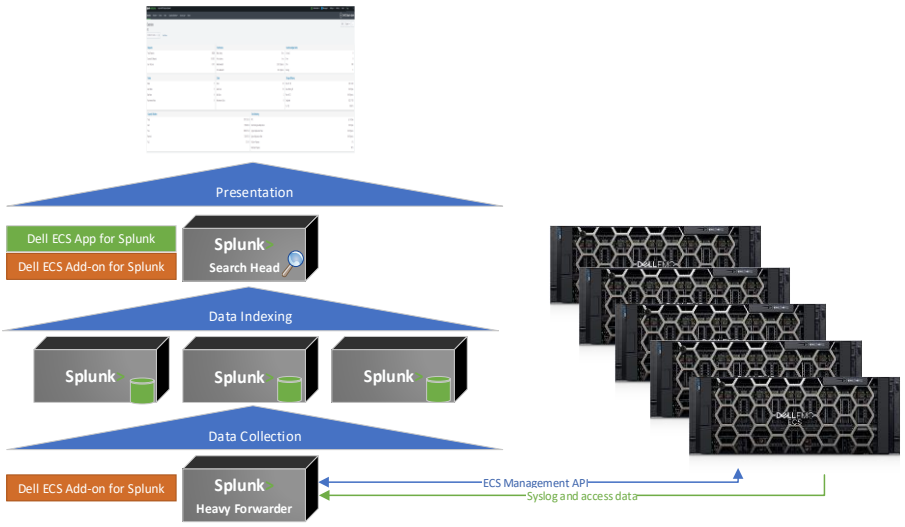


Figure 1 High-Level Architectural diagram

1.2 Solution Requirements

The following requirements must be met before installing the Technology Add-on and App.

Table 1 Requirements

Requirement	Description
ECS	Release 3.3.x and above
Splunk Enterprise	Version 7.1.x, 7.2.x and 7.3.x

1.3 Dashboards

The Dell EMC ECS App for Splunk Enterprise includes several dashboards that present data collected from ECS. The below table illustrates the reporting levels and sub-menus.

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 sub-menu dashboards that display data access metrics

1.4 Prerequisites

Please be aware of the following prerequisites before installing the Splunk App for ECS.

Port Access

This app utilizes the ECS Management API which communicates on port 4443. This port will need to be opened for the Add-on to collect metrics from the ECS VDC.

Data Access Logs

An RPQ will need to be submitted to configure rsyslog on the ECS VDC. This is so data access logs can be forwarded to the Splunk heavy forwarder of indexers. Please contact your local account teams to submit the RPQ on your behalf.

Note: These changes will not persist post OS upgrades. The Customer must take responsibility to manage the settings after an upgrade

ECS Management User

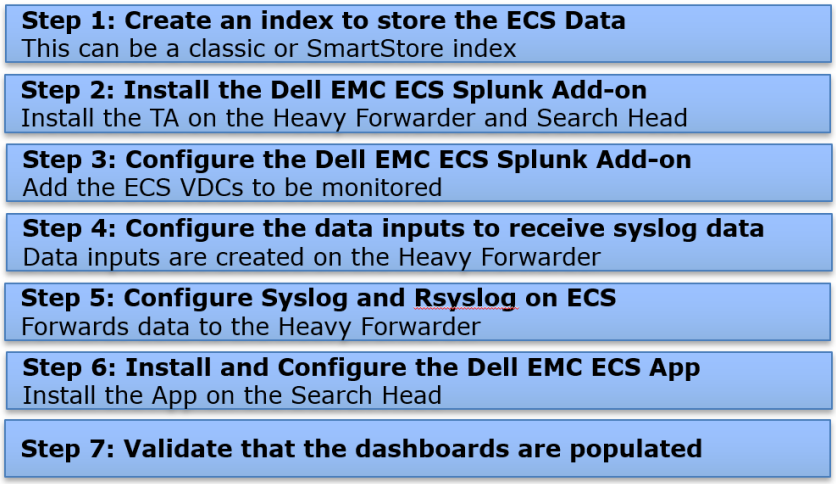
We recommend creating a Management User from the ECS Web Portal with read-only (system monitor) privileges.

2 Solution implementation

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

2.1 Implementation workflow

The below workflow illustrates the steps covered in the below Installation and Configuration section.



2.2 Installation and Configuration steps

2.2.1 Create an Index to store ECS Data

An existing Splunk index can be used to store the incoming data from ECS however it's recommended to create a new one. The index can be a SmartStore or Non-SmartStore index.

Note: If using a Heavy Forwarder, then the same index name must also be created on it.

Reference this document to create a SmartStore index with ECS.

2.2.2 Install the Dell EMC 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 using from the UI

1. Log in to Splunk Web and navigate to Apps > Manage Apps.
2. Click `install app from file`.
3. Click `Choose file` and select Dell EMC ECS Add-on installation file.
4. Click on `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. Unpack the file using “tar xvzf <name of ECS TA package> -C /$SPLUNK_HOME/etc/apps/
4. Restart Splunk

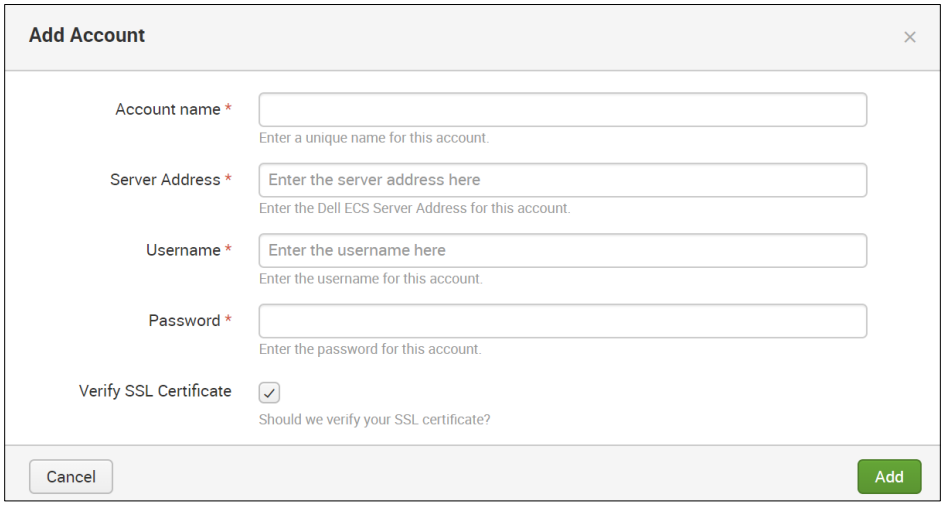
2.2.3 Configure the Dell EMC ECS Splunk Technology Add-on

Once Splunk has restarted, login 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 on the `Configuration` tab next to `Inputs` tab.
2. Click on 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.
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.

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

Create an account for each ECS VDC.

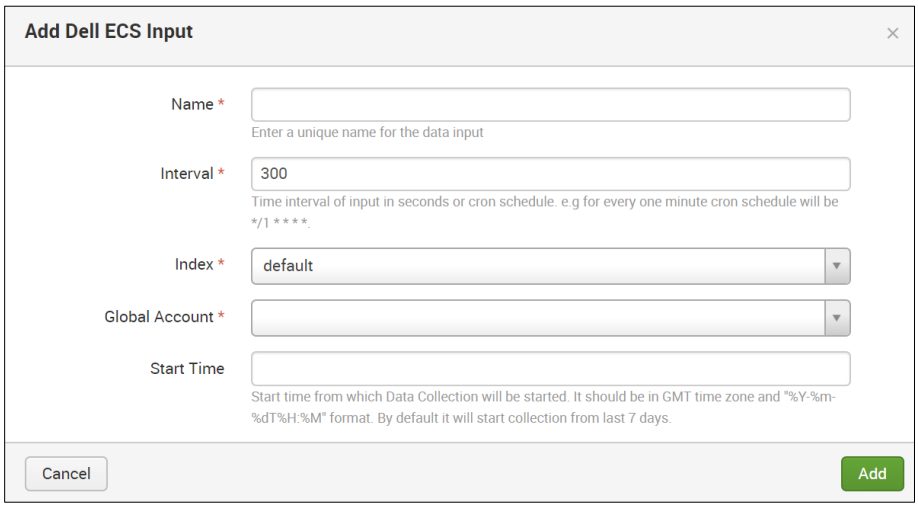
Inputs Tab

1. Click on `Create New Input` button from the 'Inputs' tab.
2. Multiple inputs are required for each ECS VDC
   - `Dell ECS Input` will index all the data into the Splunk except Namespace and Bucket data.
   - `Dell ECS Namespace Input` will index Namespace data only.
   - `Dell ECS Buckets Input` will index 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, in the case there are several namespaces, one may choose to set the interval in the Dell ECs Namespace Input to once per day to limit the number of API calls that are executed.

3. Create each input for each ECS VDC



Name: Enter a unique name for the Input (i.e. VDC1, VDC1_Namespace, VDC1_Buckets)
Interval: Keep the default or enter a new interval
Index: Select the index to store the ECS data (Should be the one created in Section 2.2.1)
Global Account: This should correspond to the VDC that is created in the 'Configuration' tab.
Start Time: (Optional) Specify when Data Collection should start

2.2.4 Configure data Inputs to receive syslog and access data from the ECS VDCs

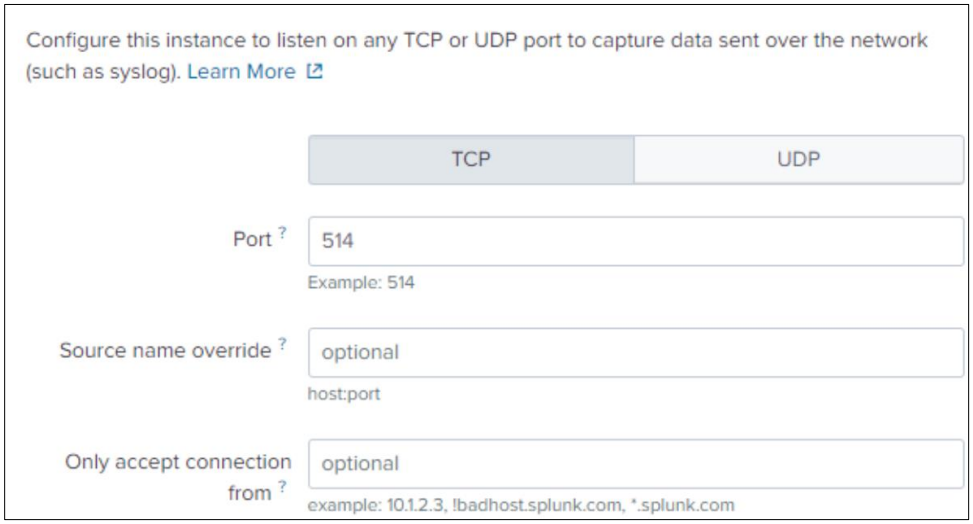
Create Data Inputs on the Heavy Forwarder to receive syslog and data access logs from ECS.

Syslog Forwarding

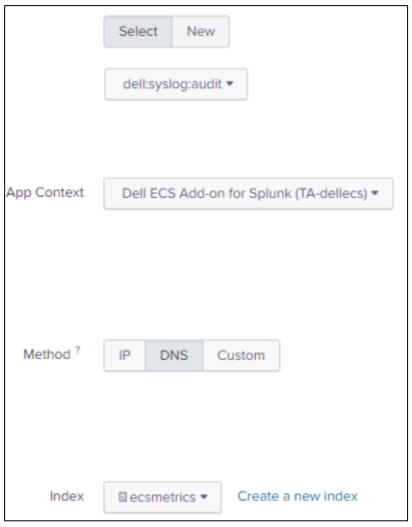
The following example configures a Data Input to receive syslog data from ECS to the Heavy Forwarder using the TCP protocol.

1. Select **TCP** from the Data inputs menu
2. Select the '**New Local TCP**' button at the top right-hand corner of the page

3. Enter the port the forwarder will be listening on and optionally override the source name (default will be tcp:<port>) and connections to accept. Click '**Next**'



4. Click the '**Next**' button
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. Note: This should be the same index the collector is using to store ECS data

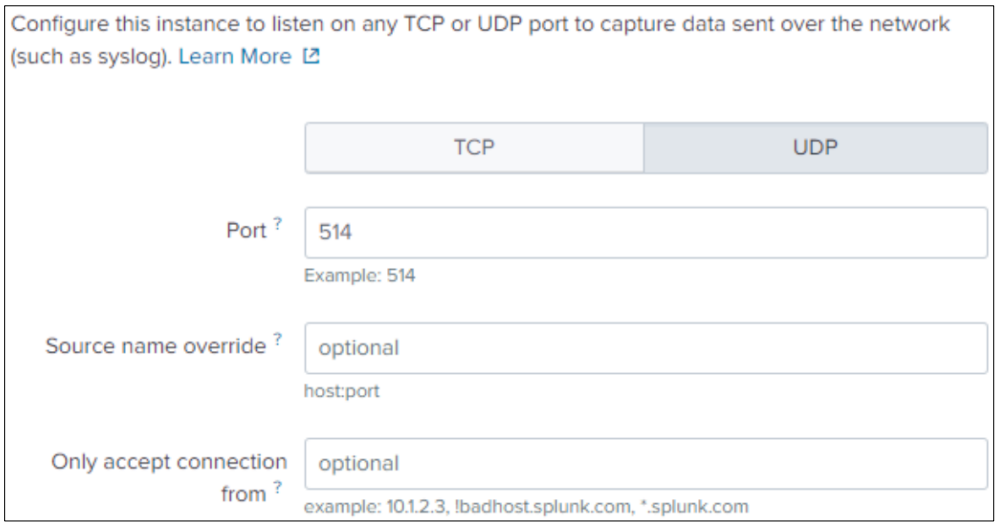


6. Click the '**Review'** button to review the setup and then '**Submit**'.

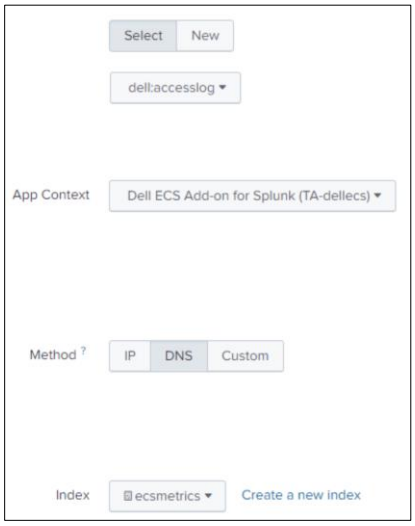
Access Log Forwarding

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

1. Select **UDP** from the Data inputs menu
2. Select the '**New Local UDP**' button at the top right-hand corner of the page
3. Enter the port the forwarder will be listening on 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. Note: This should be the same index the TA is using to store ECS data

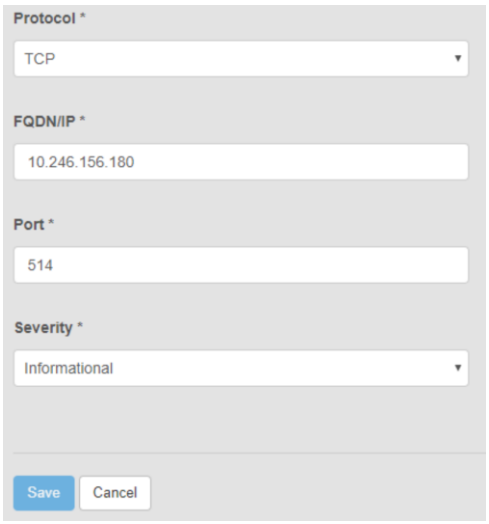


5. Click the '**Review'** button to review the setup and then '**Submit**'.

2.2.5 Configure syslog and rsyslog on the ECS VDCs

Configure ECS to forward syslogs to the Heavy Forwarder

1. Login to the ECS Web Portal and navigate to **Settings>Event Notifications>Syslog**
   a. Select the '**New Server**' button
   b. Select the Protocol. (Must match the protocol defined in the Splunk Data input which 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 which was previously created.)
   e. Enter the severity



2. Click the '**Save**' button

Configure ECS to forward Data Access logs to the Heavy Forwarder

Note: An RPQ must be requested to configure rsyslog on the ECS VDC. Please contact your local account teams to submit the RPQ on your behalf.

The below example is a rsyslog configuration file that can be used with ECS to forward data access logs to the Spunk Heavy Forwarder.

Example rsyslog configuration file

```
module(load="imfile" mode="polling" PollingInterval="10")

ruleset(name="ecss3accesslogs") {
action(type="omfwd" Target="10.246.156.180" Port="514" Protocol="udp")
stop
}

input(type="imfile" ruleset="ecss3accesslogs"
File="/opt/emc/caspian/fabric/agent/services/object/main/log/dataheadsvc-access.log"
Tag="ecss3"
Severity="info"
Facility="local7")
```

Note that 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 will not persist post OS upgrades. The Customer must take responsibility to manage the settings after an upgrade

2.2.6 Install and Configure the Dell EMC 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 using from the UI

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

Install from the CLI

5. Transfer the App package to the Search Head
6. SSH to the server
7. Unpack the file using “tar xvzf <name of ECS App Package> -C /$SPLUNK_HOME/etc/apps/
8. Restart Splunk

Configure the Base value

1. Navigate to Apps > Manage Apps.
2. Filter `Dell ECS App for Splunk` and click `Set up` under the Actions.
3. Setup the base value and click `save`.

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

Configure the index name for the Macro

1. Navigate to Settings > Advanced search > Search macros.
2. Filter for `Dell_ECS_index` and click `Dell_ECS_index` under the name.
3. Edit the macro definition `(index = <index name>)`.

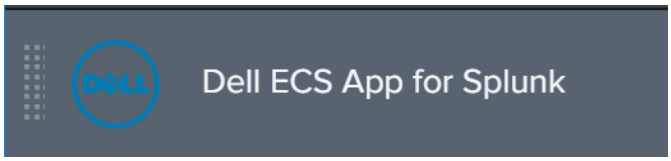
Note:This should be the same index that was created in Section 2.2.1 and used to configure the Technology Add-on.

4. Click `Save`.

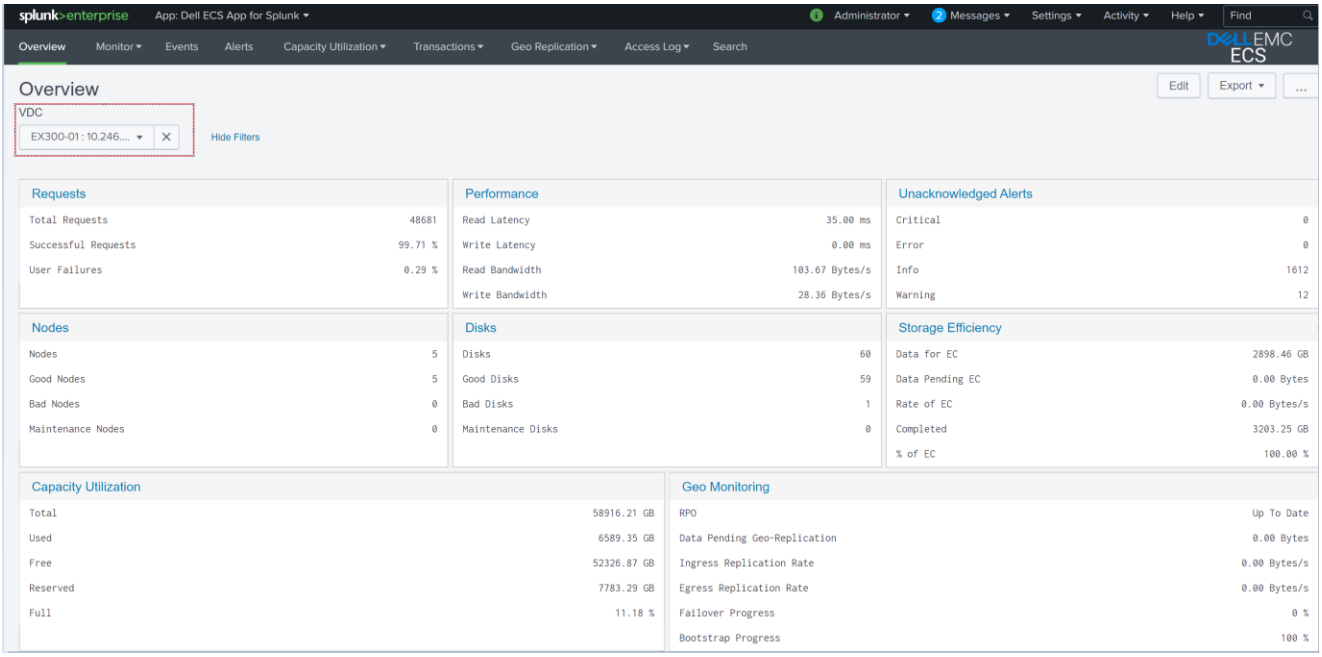
2.2.7 Validate that data is getting collected

To view the data that's being logged by the `Dell EMC ECS Add-on for Splunk`, select the `Search` tab and search for the ``Dell_ECS_index`` macro.

Navigate to the Splunk App for ECS on the Splunk Search Head where the app was installed and click on the Application.



Verify that each VDC which was configured is displayed in the 'VDC' Dropdown.



Note: Data Collection for the overview page looks back 24 hours so data may not be displayed right away.

If dashboards are not getting populated then frm the search head, navigate to settings > Searches, Reports, and Alerts and run the `dell_vdc_list` saved search.

A Technical support and resources

Please email us at dell-support@crestdatasys.com for support or questions regarding the add-on and/or app.