SL1 Operational Insights – Platform Operations v103

This PowerPack provides Operational Insights into Platform Operations for the SL1 platform.

NOTE: This PowerPack requires that all ScienceLogic Appliances to be discovered as monitored devices. It is also required that all Data and Message Collector device names match with the Data and Message Collector Appliance names from the Appliances page (System > Settings > Appliances).

NOTE: For HA or HA+DR systems the HA VIP should be discovered as a separate device.

The PowerPack contains

- **2 x Dynamic Application**
- **4 x Dashboards**
- **8 x Widgets**
- **1 x Credential**

PowerPack Installation

Following step by step instructions will ensure that you install the PowerPack successfully.

1. Navigate to System > Manage > PowerPacks
2. Select Actions > Import Powerpack
3. Select the PowerPack file and Import
4. Once imported click on the Install button

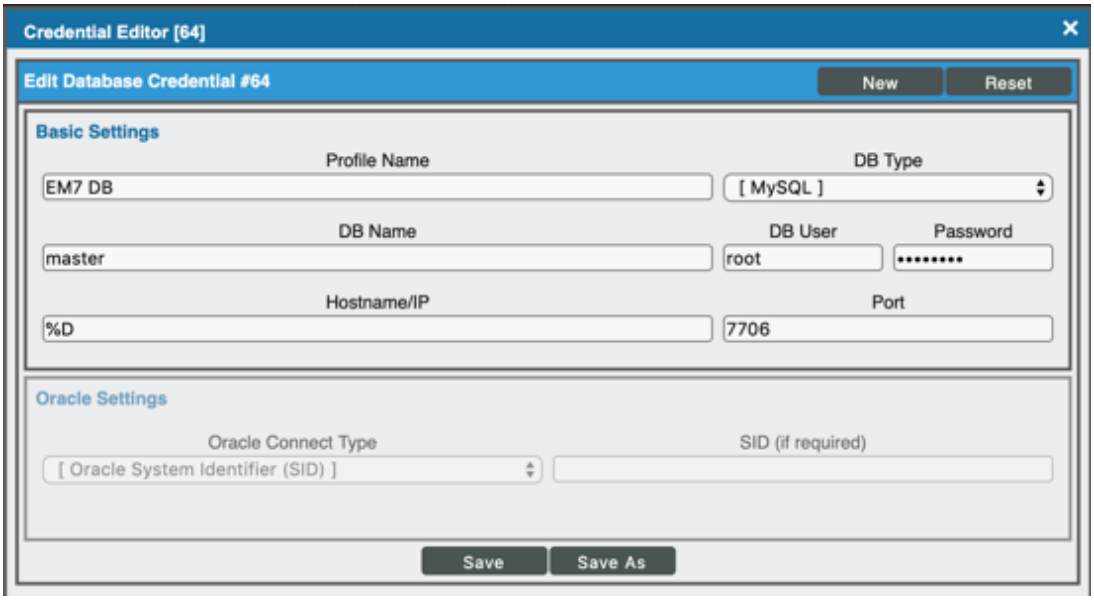
The PowerPack should now be installed on the system.

Dynamic App Installation

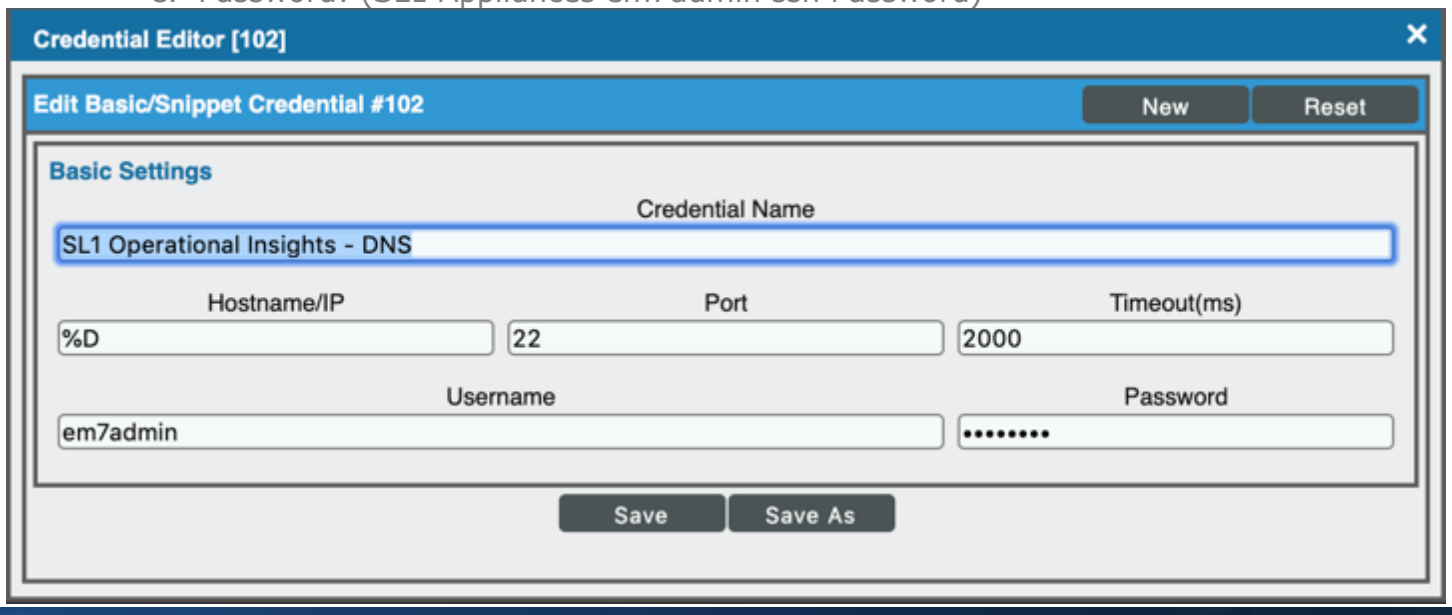
The installation of the PowerPack also requires a manual alignment of the Dynamic Application to the Primary DB.

1. Navigate to the Device Manager under Registry > Devices > Device Manager
2. Search for the Primary SL1 DB
3. Click on the wrench for the Primary DB
4. Navigate to the Collections Tab on the Primary DB
5. Select Actions > Add Dynamic Application
6. Search for **SL1 Operational Insights - Event Counts By Severity** under Dynamic Applications
7. Select a Database Credential (EM7 DB) – if no DB credential is available create a new DB credential with the following options:
    a. DB Name: master
    b. DB User: root
    c. Password: MariaDB Password
    d. Hostname/IP: %D

e. Port: 7706



8. Click Save
9. The following should be applied to all SL1 appliances in the system. Either by using a Device Template or by individually aligning the app with the SL1 appliances.
10. Select Actions > Add Dynamic Application
11. Search for **SL1 Operational Insights - DNS/Timeservers Auditing** under Dynamic Applications
12. Select a Basic Snippet Credential (**SL1 Operational Insights - DNS**) – You can use the credential that comes with the PowerPack or create your own Basic Snippet Credential with the following options:
    a. Hostname/IP: %D
    b. Port: 22 or custom ssh port if any
    c. Timeout: 2000
    d. Username: em7admin
    e. Password: (SL1 Appliances em7admin ssh Password)

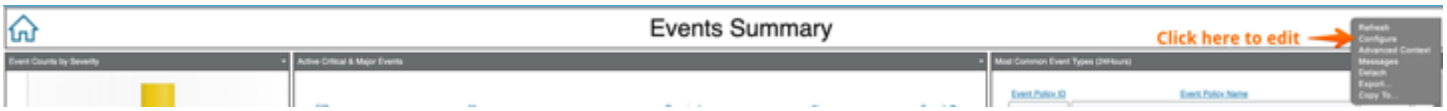


Dashboard Configuration

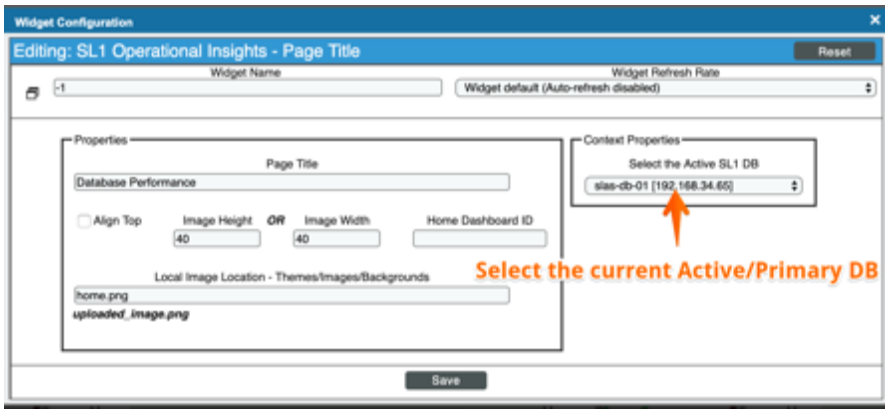
There are Dashboards that needs minor configurations. The following steps will provide the details to configure the dashboard.

Active DB Context configuration

1. Navigate to the Operational Insights Landing page and open Event Summary Dashboard
2. Edit the Top widget with the Dashboard Name and click configure:



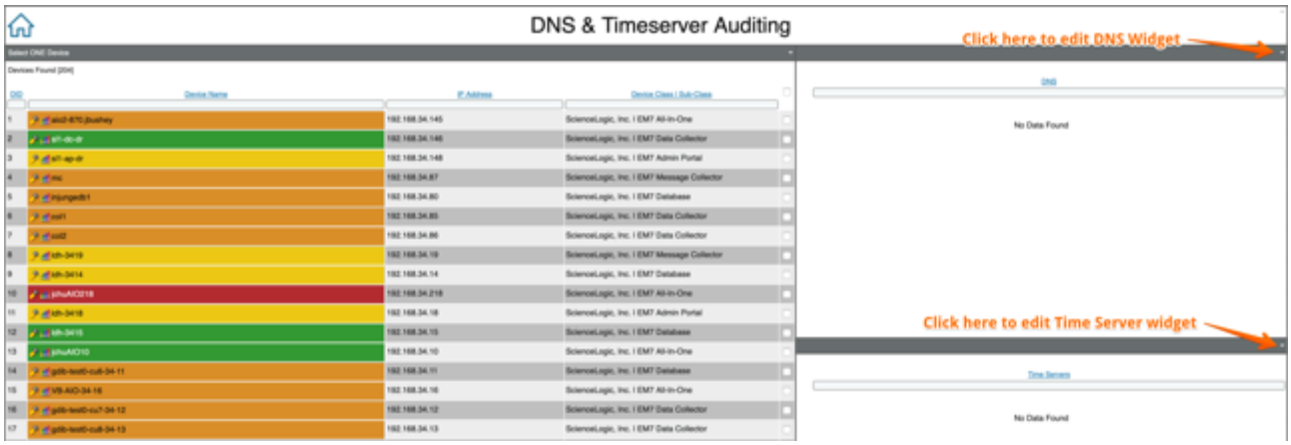
3. Select the current Active/Primary DB from the dropdown



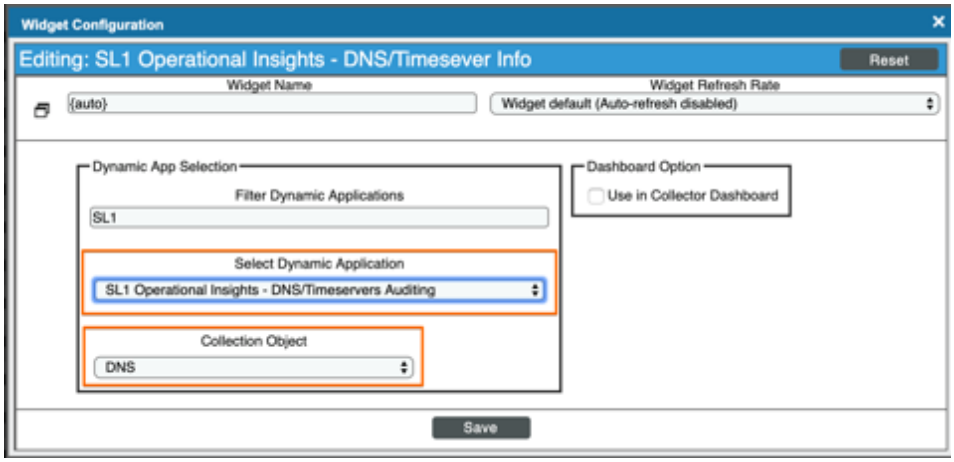
4. Click save to save your changes and exit.
5. Repeat Steps 1-4 for the following Dashboards:
    a. Backup Status History
    b. Data Retention Auditing
    c. DNS Time Server Auditing

DNS/Time Server Auditing Dashboard Configuration

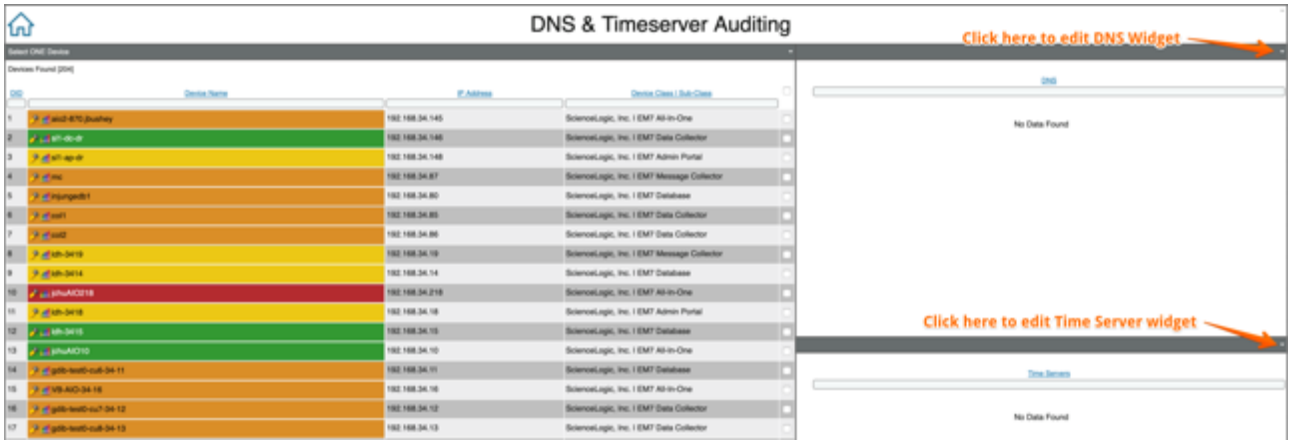
1. Navigate to the Operational Insights Landing page
2. Once the Landing Page dashboard has been configured, open the DNS Time Server Auditing Dashboard.
3. Edit the DNS Widget



4. Select the "SL1 Operational Insights - DNS/Time Servers Auditing" Dynamic Application from the drop down
5. Select "DNS" from the Collection Object dropdown.
6. Image shows the items to be selected for steps 4 and 5 highlighted in Orange.



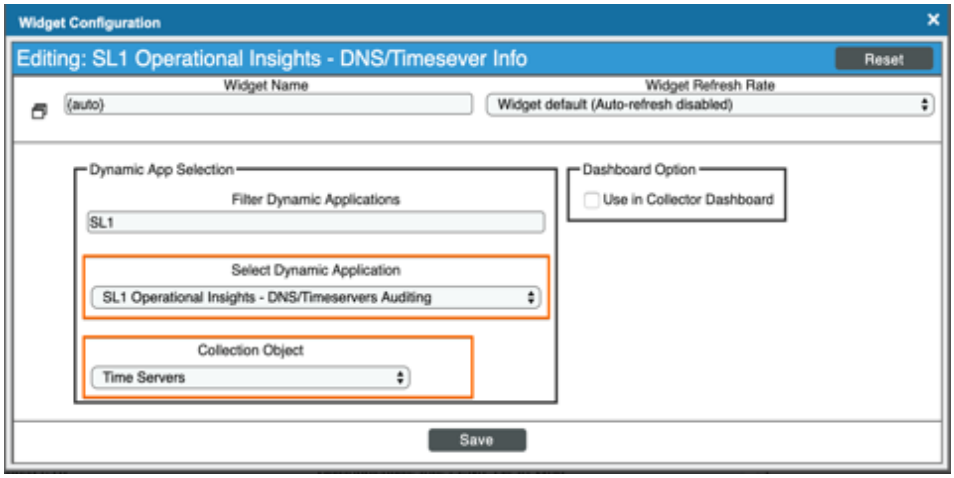
7. Click Save to save your changes and exit.
8. Edit the Time Server Widget



9. Select the "SL1 Operational Insights - DNS/Time Servers Auditing" Dynamic Application from the drop down

10.Select "Time Servers" from the Collection Object dropdown.

11.Image shows the items to be selected for steps 9 and 10 highlighted in Orange.

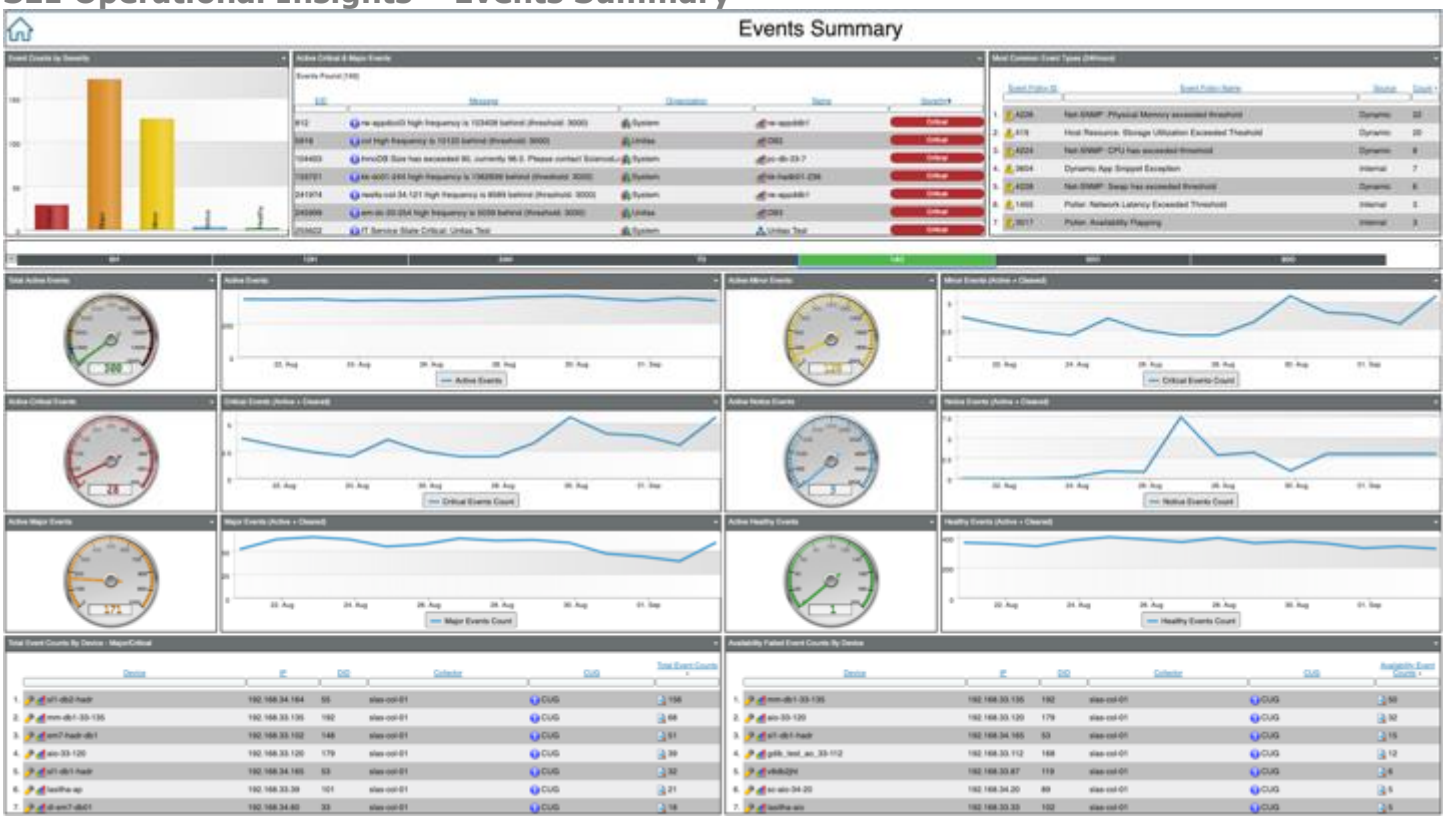


12.Click Save to save your changes and exit.

Dashboard Details

There are 4 Dashboards that are a part of the Self Monitoring PowerPack.

SL1 Operational Insights – Events Summary



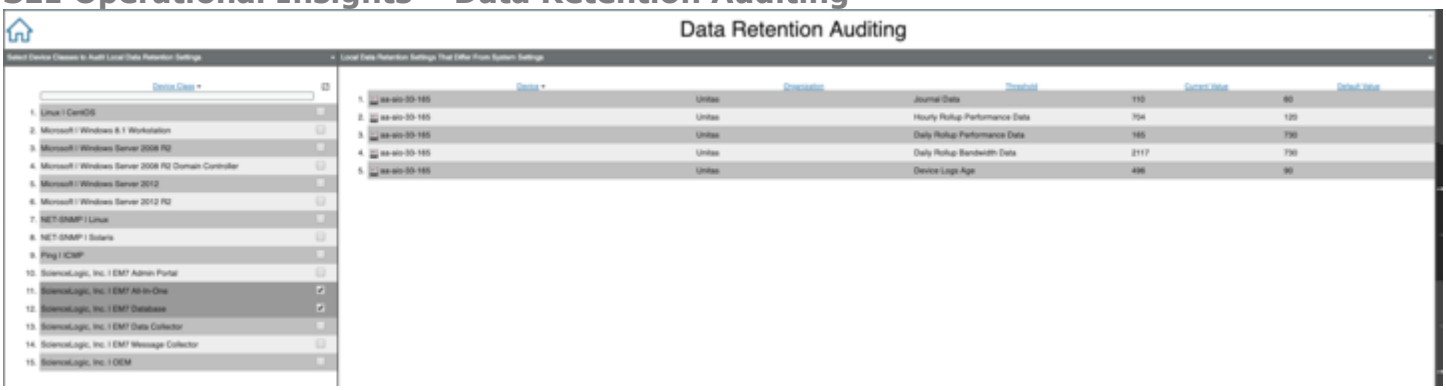
This dashboard provides a summary of all events in the system. The dashboard displays event count trends broken down by event severity. The dashboard also shows the top 10 most common events that have been triggered in the past 24 hours.

Along with the event trends, there is also information about the devices with the greatest number of Events for a selected time span. Also, there is a table that shows the devices with the greatest number of failed availability events. This information can help identify the devices that are potentially flapping a lot within the selected time span.

SL1 Operational Insights – Backup Status History

This dashboard, now also available for systems on 8.12 and higher systems, displays the status of the out of the box backup process. The dashboard shows the start and end times of the backup process along with the Duration and the last known status with any failure messages.

SL1 Operational Insights – Data Retention Auditing

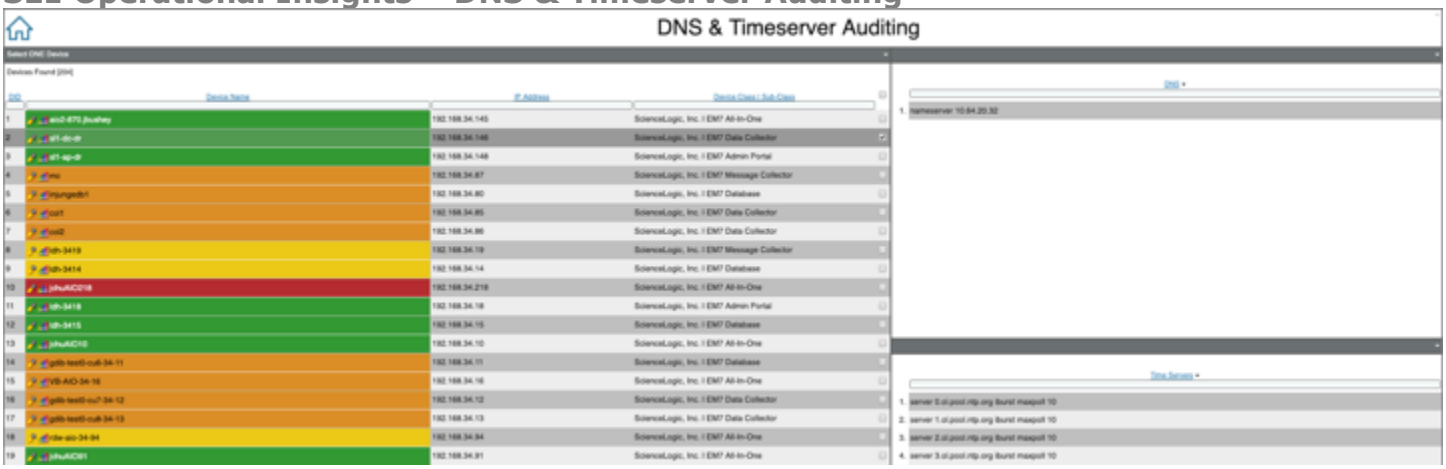


This dashboard provides a list of any devices for the selected Device Class that have their Data Retention Thresholds changed from the out of the box Defaults. Ideally the dashboard should be blank indicating that there are no devices with incorrect/changed thresholds.

Currently the only threshold that are looked at are the Data Retention Thresholds:

- Device Logs Max
- Device Logs Age
- Bandwidth Data
- Daily Rollup Bandwidth Data
- Hourly Rollup Bandwidth Data
- Raw Performance Data
- Daily Rollup Performance Data
- Hourly Rollup Performance Data
- Journal Data
- Configuration Data

SL1 Operational Insights – DNS & Timeserver Auditing



The DNS & Timeserver Auditing Dashboard allows users to audit the DNS and Timeserver settings on their SL1 Appliances.

When configured the dashboard shows the DNS and Time servers configured on the selected SL1 appliance. This information is collected using a Dynamic Application that collects the information using SSH. This can be a useful dashboard to troubleshoot any DNS or time related issues across the SL1 appliances.