

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

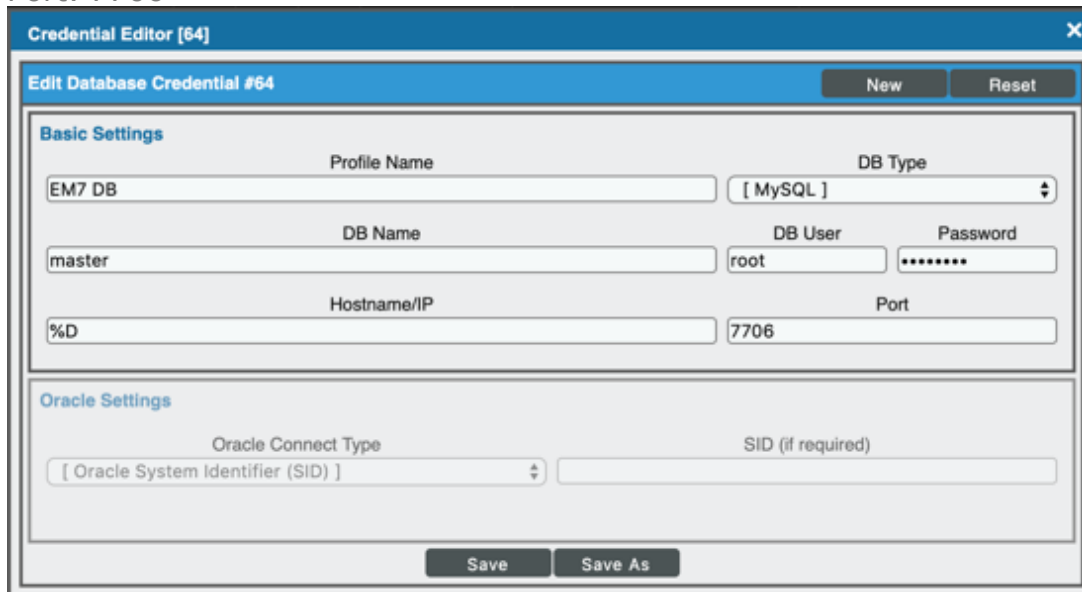
The PowerPack should now be installed on the system.

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



Credential Editor [64]

Edit Database Credential #64 New Reset

Basic Settings

Profile Name: EM7 DB DB Type: [MySQL]

DB Name: master DB User: root Password:

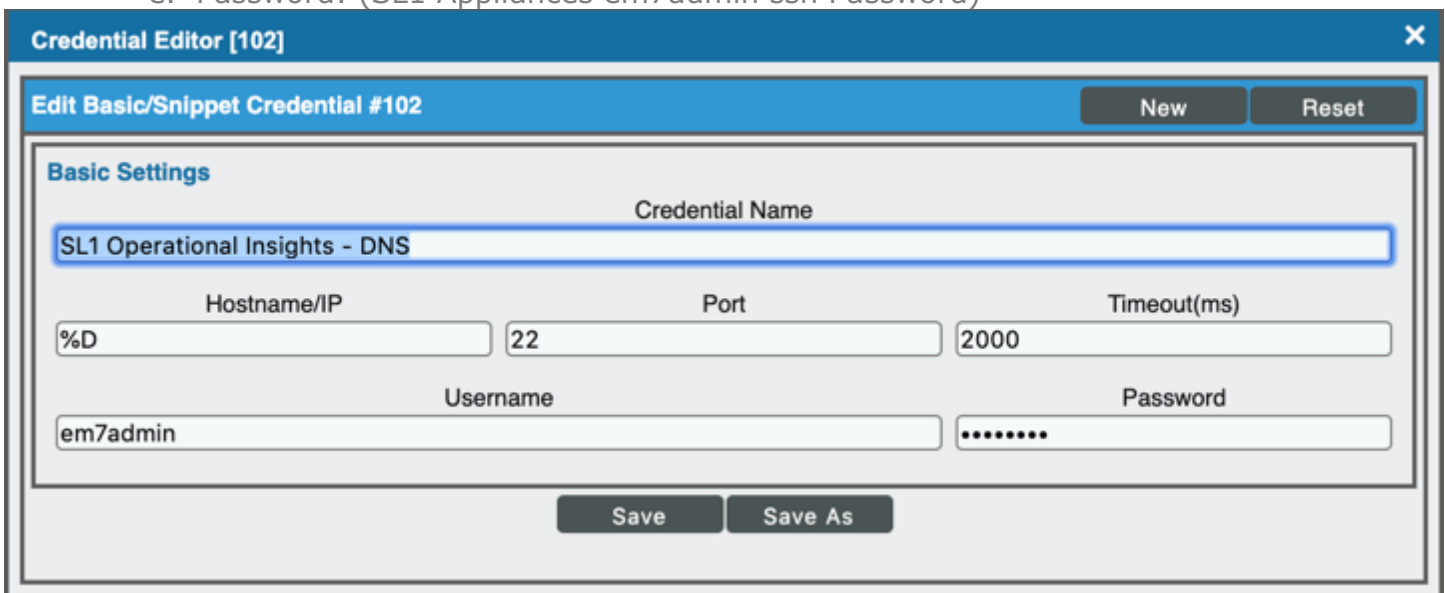
Hostname/IP: %D Port: 7706

Oracle Settings

Oracle Connect Type: [Oracle System Identifier (SID)] SID (if required):

Save Save As

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)



Credential Editor [102]

Edit Basic/Snippet Credential #102 New Reset

Basic Settings

Credential Name: SL1 Operational Insights - DNS

Hostname/IP: %D Port: 22 Timeout(ms): 2000

Username: em7admin Password:

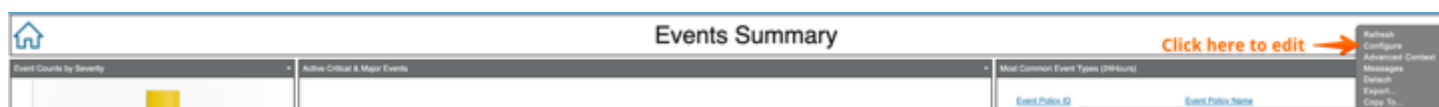
Save Save As

Dashboard Configuration

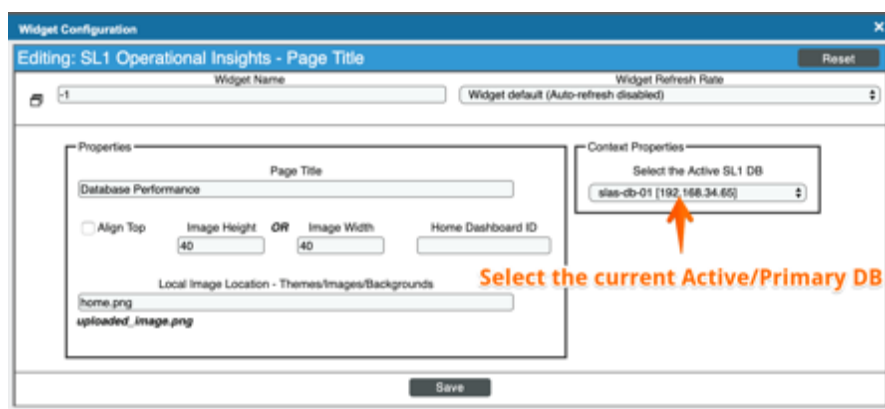
There are Dashboards that needs minor configurations. The following steps will provide the details to configure the dashboard.

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:



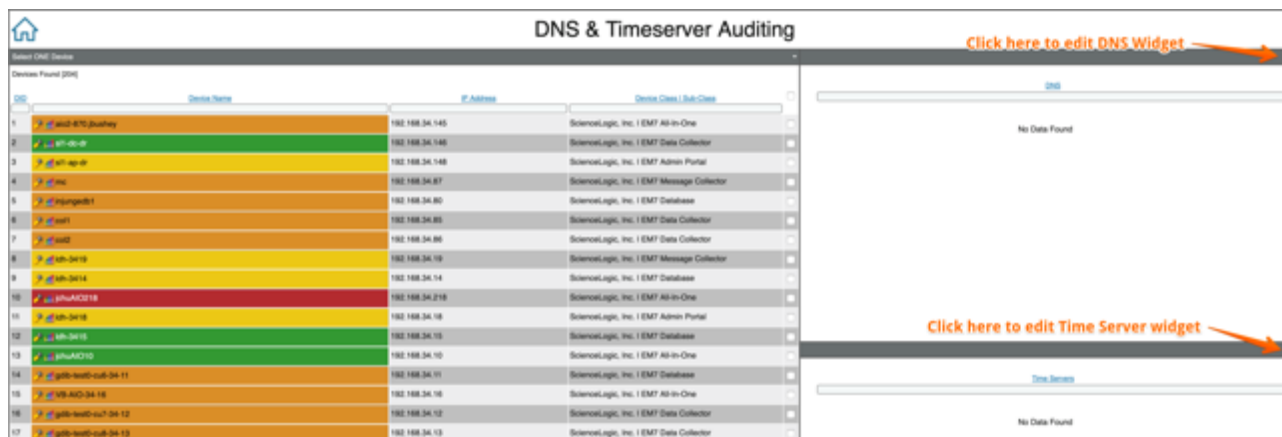
3. Select the current Active/Primary DB from the dropdown



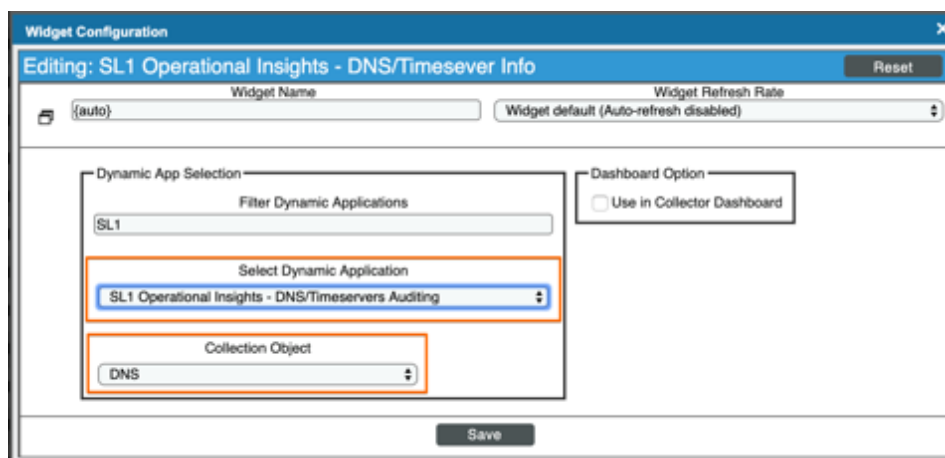
4. Click save to save your changes and exit.
5. Repeat Steps 1-4 for the following Dashboards:
 - a. Backup Status History
 - b. Data Retention Auditing
 - c. DNS Time Server Auditing

DNS/Time Server Auditing Dashboard Configuration

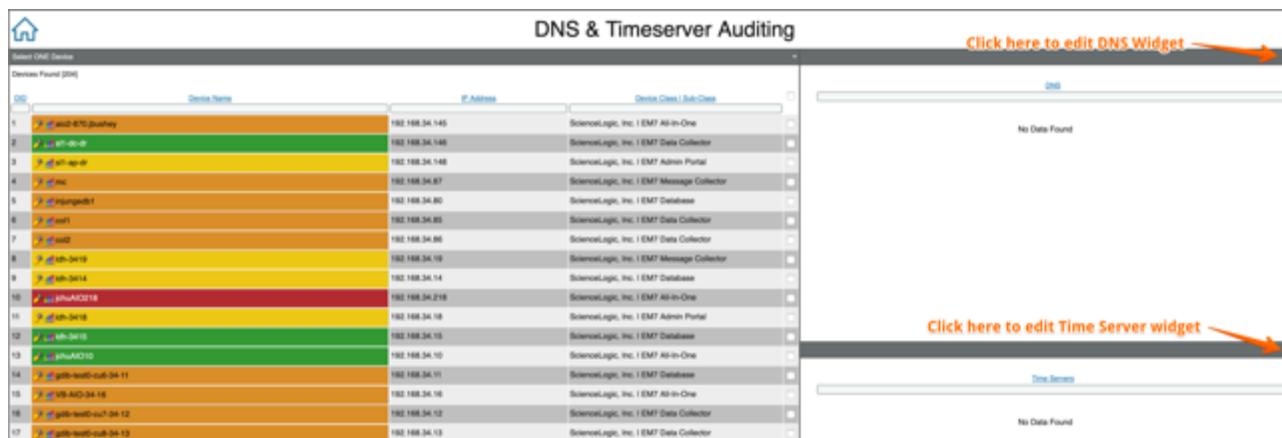
1. Navigate to the Operational Insights Landing page
2. Once the Landing Page dashboard has been configured, open the DNS Time Server Auditing Dashboard.
3. Edit the DNS Widget



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.



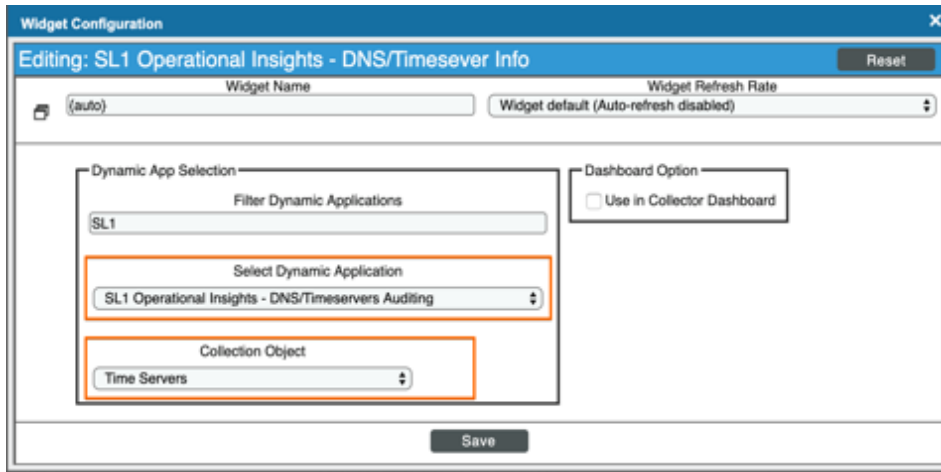
7. Click Save to save your changes and exit.
8. Edit the Time Server Widget



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.



Widget Configuration

Editing: SL1 Operational Insights - DNS/Timesever Info

Widget Name: {auto}

Widget Refresh Rate: Widget default (Auto-refresh disabled)

Dynamic App Selection

Filter Dynamic Applications: SL1

Select Dynamic Application: SL1 Operational Insights - DNS/Timeservers Auditing

Collection Object: Time Servers

Dashboard Option: ☐ Use in Collector Dashboard

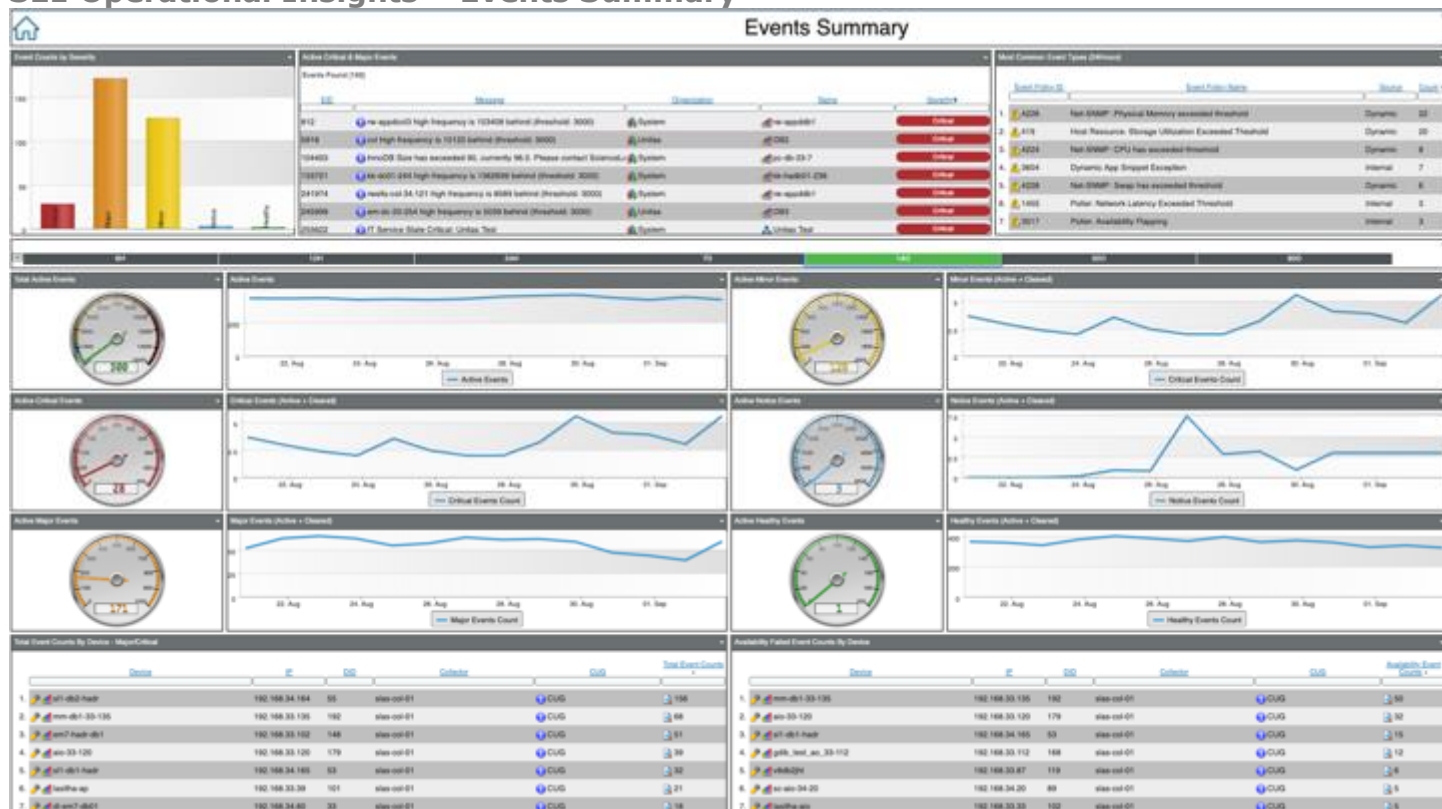
Save

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

Backup Status						
Configuration & Full Backup Status History						
	Backup Type	Start Time	End Time	Duration	Status	Notes
1.	Configuration	2019-09-02 17:45:11	2019-09-02 17:50:51	5m 40s	Successful	Backup process completed
2.	Full	2019-09-02 17:30:12	2019-09-02 17:30:13	5m 0s	Failed	Backup error - insufficient space to perform backup

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

Data Retention Auditing						
Select Device Classes to Audit Local Data Retention Settings						
Local Data Retention Settings That Differ From System Settings						
Device Class	Device	Configuration	Threshold	Current Value	Default Value	Default Value
1. Linux / CentOS	66-40-35-185	Unitas	Journal Data	110	90	
2. Microsoft / Windows 8.1 Workstation	66-40-35-185	Unitas	Hourly Rollup Performance Data	704	120	
3. Microsoft / Windows Server 2008 R2	66-40-35-185	Unitas	Daily Rollup Performance Data	165	700	
4. Microsoft / Windows Server 2008 R2 Domain Controller	66-40-35-185	Unitas	Daily Rollup Bandwidth Data	2117	700	
5. Microsoft / Windows Server 2012	66-40-35-185	Unitas	Device Logs Age	496	90	
6. Microsoft / Windows Server 2012 R2						
7. NET-SNMP / Linux						
8. NET-SNMP / Solaris						
9. Ping / ICMP						
10. ScienceLogic, Inc. / EM7 Admin Portal						
11. ScienceLogic, Inc. / EM7 All-in-One						
12. ScienceLogic, Inc. / EM7 Database						
13. ScienceLogic, Inc. / EM7 Data Collector						
14. ScienceLogic, Inc. / EM7 Message Collector						
15. ScienceLogic, Inc. / DEM						

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

DNS & Timeserver Auditing			
Select One (None)			
Devices Found (20)			
SL1	Device Name	IP Address	Device Class / Sub-Class
1	sl1-470-jwdfey	192.168.34.145	ScienceLogic, Inc. EMT All-in-One
2	sl1-470-jwdfey	192.168.34.146	ScienceLogic, Inc. EMT Data Collector
3	sl1-470-jwdfey	192.168.34.148	ScienceLogic, Inc. EMT Admin Portal
4	sl1-470-jwdfey	192.168.34.87	ScienceLogic, Inc. EMT Message Collector
5	sl1-470-jwdfey	192.168.34.80	ScienceLogic, Inc. EMT Database
6	sl1-470-jwdfey	192.168.34.85	ScienceLogic, Inc. EMT Data Collector
7	sl1-470-jwdfey	192.168.34.86	ScienceLogic, Inc. EMT Data Collector
8	sl1-470-jwdfey	192.168.34.19	ScienceLogic, Inc. EMT Message Collector
9	sl1-470-jwdfey	192.168.34.14	ScienceLogic, Inc. EMT Database
10	sl1-470-jwdfey	192.168.34.218	ScienceLogic, Inc. EMT All-in-One
11	sl1-470-jwdfey	192.168.34.18	ScienceLogic, Inc. EMT Admin Portal
12	sl1-470-jwdfey	192.168.34.15	ScienceLogic, Inc. EMT Database
13	sl1-470-jwdfey	192.168.34.10	ScienceLogic, Inc. EMT All-in-One
14	sl1-470-jwdfey	192.168.34.11	ScienceLogic, Inc. EMT Database
15	sl1-470-jwdfey	192.168.34.16	ScienceLogic, Inc. EMT All-in-One
16	sl1-470-jwdfey	192.168.34.12	ScienceLogic, Inc. EMT Data Collector
17	sl1-470-jwdfey	192.168.34.13	ScienceLogic, Inc. EMT Data Collector
18	sl1-470-jwdfey	192.168.34.84	ScienceLogic, Inc. EMT All-in-One
19	sl1-470-jwdfey	192.168.34.91	ScienceLogic, Inc. EMT All-in-One

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.