SL1 Acropolis 8.10.1 Release Notes

SL1 version 8.10.1.3

Table of Contents

Overview

This document describes:

- The *Issues Addressed* in the 8.10.1.3 release
- The *Issues Addressed* in the 8.10.1.2 release
- The *Issues Addressed* in the 8.10.1.1 release
- The *New Features* in the 8.10.1 release
- The *Issues Addressed* in the 8.10.1 release
- The *New Features* in the new user interface
- *Issues Addressed* in the new user interface
- The *Beta Features* available with the 8.10.1.3 release
- *Disabling the Knowledge Base*
- *Special Upgrade Process for FIPS-Compliant Systems*
- *Special Considerations for Systems Running 8.4.1 or Earlier*
- *Upgrade Process for 7.x Systems*
- *Upgrade Process for Systems Running 8.4.0 and Later*
- *Upgrading MariaDB*
- *Manual Updates for 8.1.x Systems Updated to 8.10.1.3*
- *Rebooting Appliances*
- The *features deprecated* in the 8.10.1.3 release
- The *known issues for the 8.10.1.3 release*

> **WARNING:** *If you have not previously installed 8.10.1 and then rebooted all appliances, you must do so after installing 8.10.1.3.* If you would like assistance in planning an upgrade path that meets your security needs while minimizing downtime, please contact your Customer Success Manager.

> **WARNING:** *8.10.1.3 and does not support Data Collectors and Message Collectors running the CentOS operating system. If your system includes Data Collectors and Message Collectors running the CentOS operating system, contact your Customer Success Manager for details on upgrading Data Collectors and Message Collectors to Oracle Linux before installing 8.10.1.3.*

WARNING: In the installation menu, the *Select Model Type* window displays options for *Storage Node* and *Compute Node*. These options are not available for installation in 8.10.1.3.

WARNING: ScienceLogic strongly suggests you contact Customer Support or your Customer Success Manager to plan your migration from CentOS (versions of SL1 prior to 8.1.1) to 8.10.1.3.

WARNING: 7.x systems must be upgraded to 7.8.5 before the migration to the 8.10.1.3 release. Please contact your Customer Success Manager to begin a discussion on the migration plan that is appropriate for your system.

WARNING: The Knowledge Base includes known vulnerabilities for cross-site scripting and SQL injection. If you are updating from a previous installation, ScienceLogic strongly recommends that you *disable the Knowledge Base*.

WARNING: If your system is not currently running a recent release, the upgrade process includes importing multiple upgrade files. You must wait until an update file has imported successfully (i.e. the *Import Status* column displays *Complete* in both the EM7 Release pane and the ScienceLogic OS pane) before importing the next update file.

CAUTION: If you are using the new user interface, please see the section on *Issues Addressed in the New User Interface* **before upgrading to 8.10.1.3**. ScienceLogic recommends that Systems running an AP2 version earlier than 5.55.1.3 upgrade their version of AP2 before upgrading to 8.10.1.3.

CAUTION: Before installing a release, ScienceLogic recommends that you verify that recent backups are available for your system.

CAUTION: During the normal system update process, multiple processes are stopped and restarted. This might result in missed polls, gaps in data, and/or unexpected errors. ScienceLogic recommends that you always install ScienceLogic releases during a maintenance window.

> **CAUTION:** The ScienceLogic system update process starts a background process that can perform any required post-upgrade tasks. The post-patch update process is automatically stopped after 24 hours. However, depending on the size of your database as well as the version from which you are upgrading, the post-upgrade tasks can take several days to perform. If the post-patch update process is stopped after 24 hours, the process will automatically re-start and continue processing from the point at which it was stopped. If you see an event that indicates the post-patch update process was stopped, you do not need to contact ScienceLogic support for assistance until you see the same event for three consecutive days.

> **TIP:** Before you install a ScienceLogic release, ScienceLogic recommends reviewing the hardware specifications of all the appliances in your system to ensure they meet the requirements for the current usage of your system. For more information, see https://portal.sciencelogic.com/portal/system-requirements.

> **TIP:** ScienceLogic regularly uploads new and updated PowerPacks to the Customer Portal before packaging those PowerPacks in a system update file. For more information, see https://portal.sciencelogic.com/portal/powerpacks.

Issues Addressed in 8.10.1.3

The following issues are addressed in the 8.10.1.3 release:

ScienceLogic API

- Requests to the API resource */data_performance_raw/device/dynamic_app* now successfully return performance data for all devices that meet the request criteria; the request no longer limits the returned data to 20 devices or 100 devices.
- A user who is not an SL1 administrator and who is not assigned to all organizations can now view data returned by the resource *data_performance_raw/interface*.

Issues Addressed in 8.10.1.2

The following issues are addressed in the 8.10.1.2 release:

Network Interfaces

- Addressed an issue with SNMP counters for network interfaces. SL1 now monitors the 64-bit counter (instead of a 32-bit counter) for an interface only if all the following are true: a 64-bit counter is present; and the 64-bit counter returns non-zero. If you have experienced issues where counters are misclassified, those counters will be classified correctly when you upgrade to this release and later releases.

- Addressed an issue with CBQoS metrics for network interfaces. In the Performance Reports for CBQoS network interfaces, added a second formula to correctly calculate Pre-Policy Inbound Utilization in bits. Added a second formula to correctly calculate Pre-Policy Outbound Utilization in bits.

SNMP Collection

- Addressed an issue with collection in SNMP Dynamic Applications. On devices where PDU Packing is enabled, collections that return an empty list for an OID or no value for an OID will no longer cause collection to loop indefinitely.

Issues Addressed in 8.10.1.1

The following issues are addressed in the 8.10.1.1 release:

Devices

- Addressed an issue with storage classes for device availability. The issue caused SL1 systems to be flooded with events for "Storage Object Failure" after update from 8.10.0 to 8.10.1.

New Features in 8.10.1

8.10.1 includes the following new features:

Access Hooks

- Deprecated the Access Hook "Cred:Passwords". Added two new Access Hooks to provide more granular access: "Cred: Passwords: Edit" and "Cred: Passwords: View".

Platform

- Added tools to automate configuration that allows the agent to communicate with SL1 (streamer).
- Multiple security updates including updates to the kernel, Open SSL, nss, modprobe, and glib.

Scheduled Maintenance

- In the Device Manager page (Registry > Device > Device Management), you can disable scheduled maintenance mode for one or more devices.

Scheduled Tasks

- In the ScienceLogic API, improved validation for the task resource (scheduled tasks)

Issues Addressed in 8.10.1

The following issues are addressed in the 8.10.1 release:

Collection

- Addressed an issue with Data Collection for Interface Bandwidth data. The process "Data Collection: Interface Bandwidth" (if_collect.py) no longer triggers the unhandled exceptions stating "Lock wait timeout exceeded" during collection on busy Data Collectors.

- Addressed an issue with SNMP collection. Rebuilt net-snmp packages to address an error. Users can now successfully perform SNMP queries again the object "hrSWInstalledTable".

Custom Tabs

- When Creating a Tabbed Application Form in the Application Forms page (System > Customize > Form Fields > Create), with a Form Type of "Asset", you can now include multiple, consecutive capital letters in the Description field.

Device Management

- Addressed am issue with device management. When a device property is edited, SL1 no longer stores the date and time of the change (edit_date column) in local format in the central database, but instead stores the date and time in UTC.

- Increased the frequency with which SL1 updates the IP address of each hostname-discovered (DHCP) device.

Discovery

- Addressed an issue with interface discovery using SNMP. When the discovery process finds an incorrect OID for an interface, instead of causing an unhandled exception and ending discovery, the discovery process will continue discovering interfaces and display an error message that lists which interfaces were skipped due to errors.

Multi-Tenancy

- When creating a new asset record, in the Asset Properties page users can view only organization to which they are a member and devices in those organization. Users can no longer view all devices in the system from the Asset Properties page.

Platform

- Addressed an issue with normalization of performance data. Performance data for file systems is now normalized (hourly and daily) successfully even if the data includes null values.

Run Book Automation

- Addressed an issue with Run Book Automation. To improve the performance of the Automation Engine, sub-processes are now monitored more frequently.

- Addressed an issue with Run Book Automation. If a worker process for the Automation Engine fails, SL1 no longer generates an unhandled exception and the Automation Engine no longer crashes. Instead, the worker process is automatically restarted within 20 minutes.

Scheduled Maintenance

- Addressed an issue with Scheduled Maintenance. When defining Scheduled Maintenance for a device group, you can now successfully enable Collection Polling.

Software Inventory

- Addressed an issue with Software Inventory. Fixed a bad query that was causing an unhandled exception from the process "Enterprise Database: Software Title inventory updater" (software_inventory_update.py).

New Features in the New User Interface

The following list is an overview of the features included in the new user interface. For more details, see the *Introduction to the New User Interface* manual, or launch the online help from the new user interface by clicking the "?" icon and then selecting *Help*.

> **TIP:** To identify the version of the new user interface for SL1 you have installed, click the question-mark icon in the top right-hand corner and select *About*. Locate the ap2 value in the list of ScienceLogic components in the right-hand pane.

Version 8.10.1 of the new user interface includes the following features:

Business Services

- To add an icon to a service, users can click the Assign Icon in the Inventory > Services action menu.

Dashboards

- In a Dashboard, in the Table widget, selecting a parent device displays information about the child devices.
- In a Dashboard, users can now use the Leaderboard or Table widget to display additional interface properties.
- Options for the Leaderboard and Forecast widget will appear only if these widgets have been selected.

Device Categories and Device Classes

- Users can bulk-assign an icon to multiple device categories.
- Users can bulk-assign icons to multiple device classes.

Issues Addressed in the New User Interface

If a system has been upgraded to 8.10.1 via **Content Management** and AP2 version is earlier than 5.55.13, AP2 will not start after upgrading to 8.10.1. ScienceLogic recommends that Systems running an AP2 version earlier than 5.55.1.3 upgrade before upgrading to 8.10.1.

To determine which version of AP2 you are running:

1. Click on the question-mark icon in the upper right. Select *About*.

2. In the ScienceLogic pane, fine the value for *ap2*.

If AP2 is currently running and you have not yet updated your version of AP2:

1. On each Administration Portal and the Database Server, use the **Content Management** tab to install the latest version of AP2.

2. You can now upgrade each appliance to 8.10.1.

If AP2 will not start, perform the following steps on each Administration Portal and the Database Server:

1. Go to the console of the appliance or open an SSH session to the appliance.

2. At the shell prompt, execute the following commands:

```
sudo rm -rf /var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/
sudo systemctl restart nextui
```

3. Upgrade via GraphQL

To upgrade via GraphQL, perform the following steps on each Administration Portal and the Database Server:

1. Open a browser. Enter the following as a URL:

```
ip_address_of_ap2_system/gql
```

2. In the left pane of the GraphiQL page, enter the following:

```
mutation ap2
   {
     upgradeNodePackage(name:"@sciencelogic/ap2" version:"5.64.1"){name version}
   }
mutation wc
   {
     upgradeNodePackage(name:"@sciencelogic/widget-components" version:"2.133.2")
     {name version}
   }
```

3. Click the arrow button.

4. You can now upgrade each appliance to 8.10.10.

Beta Features

The following beta features are included in the 8.10.1.3 release:

- **Manual Device Discovery**

  - This beta feature allows monitored devices to be added manually instead of via a discovery session.

- *Run Book Actions: Custom Action Type*

    - A Run Book Action of type "Custom Action Type" executes a reusable snippet. Unlike the Action Type "Snippet", a Custom Action Type can accept input parameters (in a JSON format) and create output (in a JSON format). A Custom Action Type allows a single snippet to be used in multiple Action Policies, each time with different inputs and different outputs. A Custom Action Type is associated with an Execution Environment. An Execution Environment contains the supporting modules and code (Content Libraries) required by the Custom Action Type. Content Libraries allow snippet developers to isolate the "heavy weight", re-usable code and write "light weight" snippets that call the Content Libraries.

- **PowerPacks**: Beta versions of the following PowerPacks are available. You can download then from the Customer Portal and import them into SL1:

    - Alibaba Cloud: Aliyun

    - AMQP: RabbitMQ

    - Cisco: ACI Multi-Site Manager

    - Cisco: Cloud Center

    - Cisco: Contact Center Enterprise

    - Cisco: Hyperflex

    - Cisco: Medianet/Mediatrace

    - Cisco: Meraki (API)

    - Cisco: Tetration

    - Cisco: UC Ancillary PowerPack. Includes Dynamic Applications for monitoring Cisco CUBE devices.

    - Cisco: UCS Director

    - Cisco: Unity Express (Download from the Customer Portal and Import into SL1)

    - Docker (Download from the Customer Portal and Import into SL1)

    - ELK: AWS CloudTrail

    - ELK: Azure Activity Log

    - F5: BIG-IP DNS

    - Google Cloud Platform

    - Hitachi Data Systems: VSP

    - Kubernetes

    - Link Layer Neighbor Discovery (Download from the Customer Portal and Import into SL1)

    - Microsoft: Office 365

    - Microsoft: Windows Server Event Logs

    - Palo Alto (Download from the Customer Portal and Import into SL1)

To install a beta PowerPack:

1. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).

2. Select the **[Actions]** menu and select *Install PowerPack*. The **PowerPack Installer** modal page is displayed.

3. Select the lightning-bolt icon ( ) for the PowerPack you want to install. Information about the contents of the PowerPack and the installation process is displayed.

4. Select the **[Install]** button.

> **TIP**: By default, installing an updated version of a PowerPack will overwrite all content in a PowerPack that has already been installed on the target system. You can use the *Enable Selective PowerPack Field Protection* setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields.

Disabling the Knowledge Base

The Knowledge Base includes known security vulnerabilities. ScienceLogic no longer supports the Knowledge Base

- ScienceLogic strongly recommends that existing users disable the Knowledge Base. 8.9.2 and later releases provides a new setting in the silo.conf file to disable the Knowledge Base.

- For new installations, the Knowledge Base will be disabled by default.

> **WARNING**: The Knowledge Base includes known vulnerabilities for cross-site scripting and SQL injection. ScienceLogic strongly recommends that you disable the Knowledge Base.

To disable the Knowledge Base:

1. Use SSH to connect to the Administration Portal and Database Server or All-In-One (all SL1 appliances that provide a web interface).

2. Use an editor like vi and edit the file **/etc/silo.conf.** In the LOCAL section, add the line:

   ```
   kbase_disabled=1
   ```

4. Use an editor like vi and edit the file **/etc/siteconfig/siloconf.siteconfig**. In the LOCAL section, add the line:

   ```
   kbase_disabled=1
   ```

5. Open a browser session and login to the SL1

6. From the hamburger menu ( ) in the upper right, select *Clear SL1 System Cache*.

7. Upon your next login, the Knowledge Base tab will not appear. Attempts to access the tab will result in an "Access Denied" error message.

Special Upgrade Process for FIPS-Compliant Systems

FIPS-compliant systems (those that are FIPS 140-2 enabled) should *manually upgrade to the latest version of MariaDB*.

The platform patch will automatically update MariaDB-client, MariaDB-common, and MariaDB-shared RPMs but will not update the MariaDB Server.

Special Considerations for Systems Running 8.4.1 or Earlier

> **WARNING:** *8.10.1.3 does not support Data Collectors and Message Collectors running the CentOS operating system. If your system includes Data Collectors and Message Collectors running the CentOS operating system, contact your Customer Success Manager for details on upgrading Data Collectors and Message Collectors to Oracle Linux before installing 8.10.1.3.*

8.4.2 included a new feature for Ticketing. The Note Editor for tickets includes a drop-down menu where the user can specify that the note be saved as Plain Text or HTML. Ticket notes created in the API can also be saved as Plain Text or HTML. HTML is the default format for ticket notes in both the Note Editor and the API.

This new feature required a change to the database schema that will be performed immediately after a system is upgraded to 8.4.2 or later for the first time. If your system has not been upgraded to 8.4.2 or later, this schema change will be performed after you upgrade.

During the post-patch process, all existing ticket notes will be migrated to the new schema in batches. During the migration, all ticket notes will be unavailable. The user interface and API will not display ticket notes. Ticket notes cannot be viewed or updated during the post-patch process. On a system that included 2,000,000 ticket notes, this process took approximately 6 hours.

If you require access to all ticket notes immediately after installing an 8.4.2 or later release, contact ScienceLogic Customer Support for details on manually updating the database schema before you upgrade to 8.4.2 or later.

The 8.4.2 release also changed the firewall on all appliances from iptables to firewalld. If you are currently running a release earlier than 8.4.2 and have added one or more custom firewall rules, such as a non-standard port for Phone Home Collectors, these rules must be migrated before upgrading to 8.8.1. Please contact ScienceLogic Support for more information.

Upgrade Process for 7.x Systems

> **WARNING:** *8.10.1.3 does not support Data Collectors and Message Collectors running the CentOS operating system. If your system includes Data Collectors and Message Collectors running the CentOS operating system, contact your Customer Success Manager for details on upgrading Data Collectors and Message Collectors to Oracle Linux before installing 8.10.1.3.*

> **WARNING:** 7.x systems must be upgraded to 7.8.5 before the migration to an 8.x release. Please contact your Customer Success Manager to begin a discussion on the migration plan that is appropriate for your system.

The 8.1.1 release included a complete update of the ScienceLogic appliance operating system from CentOS 5.11 to Oracle Linux. Major operating system components, including the database, web server, and High Availability/Disaster Recovery packages have been updated or replaced by new industry-standard packages.

When upgrading from version 7.8.5 to version 8.10.1.3, each appliance must first be migrated to 8.9.0 and the Oracle Linux 7.5 operating system.

Upgrade from 7.x to 8.10.1.3

> **WARNING:** ScienceLogic strongly suggest you contact Customer Support or your Customer Success Manager to plan your migration from CentOS (versions of SL1 prior to 8.1.1) to 8.10.1.3.

The following is the general process for migrating from 7.x to 8.10.1.3. This is a high-level description only. For details, contact Customer Support or your Customer Success Manager.

- The existing system must be upgraded to 7.8.5 before the upgrade.
- Run the 8.10.0 migration patch.

> **NOTE**: See the separate Migration document for detailed instructions on how to perform the migration steps. Before you migrate to 8.9.0, please contact your Customer Success Manager.

- Use the 8.10.0 ISO to reinstall all Database Servers or All-In-One Appliances. Data is migrated using a logical backup while the database on the existing system is stopped. The downtime of this operation can be mitigated in several ways depending on the current architecture.
- Use the 8.10.0 ISO to reinstall all Administration Portal appliances.

- After reinstalling all Database Servers and Administration Portals, the system is operational, can monitor devices using the PowerPacks that were included in the 7.8.5 release, and can be upgraded.

- Use the 8.10.0 ISO to reinstall all Data Collectors and Message Collectors in your system.

- The process of migrating an existing system to 8.10.0 includes multiple additional steps that will vary depending on the current architecture. Please contact your Customer Success Manager to begin a discussion on the migration plan that is appropriate for your system.

- To install 8.10.1.3, see the section on *Upgrade Process for Systems Running 8.1.1 and Later.*

PowerPacks that Require Oracle Linux Data Collectors

As of the release of SL1 8.9.0 (or earlier for some PowerPacks), the following PowerPacks must be used with a Data Collector running Oracle Linux (i.e. a Data Collector that has been reinstalled using a version 8 ISO):

- Alibaba Cloud
- Amazon Web Services
- Azure
- Cisco: ACI
- Cisco: 1000'S
- Cisco: CUCM Cisco Unified Communications Manager
- Cisco: Hyper flex
- Cisco: UC VOS Applications
- Cisco: UCS Central
- F5 Big IP
- Google Cloud Platform
- Microsoft: Active Directory Server
- Microsoft: DHCP Server
- Microsoft: DNS Server
- Microsoft: Exchange Server
- Microsoft: Exchange Server 2010
- Microsoft: Hyper-V Server
- Microsoft: IIS Server
- Microsoft: Lync Server 2010
- Microsoft: Lync Server 2013
- Microsoft: SharePoint Server
- Microsoft: SQL Server
- Microsoft: SQL Server Enhanced
- Microsoft: Windows Server
- Microsoft: Windows Server Event Logs (beta release)

- Microsoft: Windows Server Services

- OpenStack

- SMI-S

- VMWare

Features Not Currently Supported by the 8.x Releases

The following functionality that was available in previous releases is not currently available in the 8.10.1.3 release, but will be re-added in a future release:

- Configuring two All-In-One Appliances for Disaster Recovery

- Applying a patch manually with the apply_patch script

Upgrade Process for Systems Running 8.4.0 and Later

> **WARNING:** *8.10.1.3 does not support Data Collectors and Message Collectors running the CentOS operating system. If your system includes Data Collectors and Message Collectors running the CentOS operating system, contact your Customer Success Manager for details on upgrading Data Collectors and Message Collectors to Oracle Linux before installing 8.10.1.3.*

> **WARNING:** *If you have not previously installed 8.10.1 and then rebooted all appliances, you must do so after installing 8.10.1.3.* If you would like assistance in planning an upgrade path that meets your security needs while minimizing downtime, please contact your Customer Success Manager.

> **WARNING:** If your system is not currently running an 8.10 release, the upgrade process includes importing multiple upgrade files (8.4.0 > 8.5.0 > 8.6.0 > 8.7.0 > 8.8.0 > 8.9.0 > 8.10.0 > 8.10.1.3). You must wait until an update file has imported successfully (when the *Import Status* column displays *Complete*) before importing the next update file.

> **CAUTION:** If you are using the new user interface, please see the section on *Issues Addressed in the New User Interface before upgrading to 8.10.1.3.* If you upgraded your system via **Content Management** and the AP2 version is earlier than 5.55.13, AP2 will not start. ScienceLogic recommends that Systems running an AP2 version earlier than 5.55.1.3 upgrade via GQL before upgrading to 8.10.1.3.

To upgrade to the 8.10.1.3 release from an 8.4.0 or later release:

> **NOTE**: Before upgrading, ensure that:
> - Each SL1 Appliance has a valid license
> - Each Data Collector is a member of a Collector Group
> - Each Data Collector is "available" to the Database Server. To check, see the **Collector Status** page (System > Monitor > Collector Status).

1. Familiarize yourself with the *Known Issues* for this release.
2. Go to the **System Updates** page and disable automatic staging (System > Tools > Updates > Actions > Disable automatic staging).
   - If you have previously used manual staging, perform these additional steps:
     - Go to the **System Updates** page (System > Tools > Updates). Select all updates in the EM7 Releases pane and select all updates in the ScienceLogic OS pane.
     - In the *Select Action* menu, select *Unstage Update (remove staging policy override)*. Click **[Go]**.
     - For software that was previously staged with automatic staging, *Unstage Update (remove staging policy override)* does not affect staging.

> **NOTE**: For details on downloading, importing, staging, and installing system updates, see the manual **System Administration**.

3. *If you are currently running an 8.4 release*:

   - From the ScienceLogic portal, download the latest update for 8.5.0, 8.6.0, 8.7.0, 8.8.0, 8.9.0, 8.10.0, and 8.10.1.3 to a local computer. Unzip any zipped files.
   - Import the 8.5.0 system update file in the System Updates page (System > Tools > Updates > **[Import]** button). The system update file will load an update in both the EM7 Releases and the ScienceLogic OS section. You must wait until the update file has imported successfully (i.e. the **Import Status** column displays *Complete*) before importing the next update file.

- Import the 8.6.0 system update file in the System Updates page (System > Tools > Updates > **[Import]** button). The system update file will load an update in both the EM7 Releases and the ScienceLogic OS section. You must wait until the update file has imported successfully (i.e. the **Import Status** column displays *Complete*) before importing the next update file.

- Import the 8.7.0 system update file in the System Updates page (System > Tools > Updates > **[Import]** button). The system update file will load an update in both the EM7 Releases and the ScienceLogic OS section. You must wait until the update file has imported successfully (i.e. the **Import Status** column displays *Complete*) before importing the next update file.

- Import the 8.8.0 system update file in the System Updates page (System > Tools > Updates > **[Import]** button). The system update file will load an update in both the EM7 Releases and the ScienceLogic OS section. You must wait until the update file has imported successfully (i.e. the **Import Status** column displays *Complete*) before importing the next update file.

- Import the 8.9.0 system update file in the System Updates page (System > Tools > Updates > **[Import]** button). The system update file will load an update in both the EM7 Releases and the ScienceLogic OS section. You must wait until the update file has imported successfully (i.e. the **Import Status** column displays *Complete*) before importing the next update file.

- Import the 8.10.0 system update file in the System Updates page (System > Tools > Updates > **[Import]** button). The system update file will load an update in both the EM7 Releases and the ScienceLogic OS section. You must wait until the update file has imported successfully (i.e. the **Import Status** column displays *Complete*) before importing the next update file.

- Go to step #10 and continue.

4. *If you are currently running an 8.5 release*:

- From the ScienceLogic portal, download the latest update for 8.6.0, 8.7.0, 8.8.0, 8.9.0, 8.10.0, and 8.10.1.3 to a local computer. Unzip any zipped files.

- Import the 8.6.0 system update file in the System Updates page (System > Tools > Updates > **[Import]** button). The system update file will load an update in both the EM7 Releases and the ScienceLogic OS section. You must wait until the update file has imported successfully (i.e. the **Import Status** column displays *Complete*) before importing the next update file.

- Import the 8.7.0 system update file in the System Updates page (System > Tools > Updates > **[Import]** button). The system update file will load an update in both the EM7 Releases and the ScienceLogic OS section. You must wait until the update file has imported successfully (i.e. the **Import Status** column displays *Complete*) before importing the next update file.

- Import the 8.8.0 system update file in the System Updates page (System > Tools > Updates > **[Import]** button). The system update file will load an update in both the EM7 Releases and the ScienceLogic OS section. You must wait until the update file has imported successfully (i.e. the **Import Status** column displays *Complete*) before importing the next update file.

- Import the 8.9.0 system update file in the System Updates page (System > Tools > Updates > **[Import]** button). The system update file will load an update in both the EM7 Releases and the ScienceLogic OS section. You must wait until the update file has imported successfully (i.e. the **Import Status** column displays *Complete*) before importing the next update file.

- Import the 8.10.0 system update file in the System Updates page (System > Tools > Updates > **[Import]** button). The system update file will load an update in both the EM7 Releases and the

ScienceLogic OS section. You must wait until the update file has imported successfully (i.e. the **Import Status** column displays *Complete*) before importing the next update file.

- Go to step #10 and continue.

5. *If you are currently running an 8.6 release*:

- From the ScienceLogic portal, download the latest update for 8.7.0, 8.8.0, 8.9.0, 8.10.0, and 8.10.1.3 to a local computer. Unzip any zipped files.

- Import the 8.7.0 system update file in the System Updates page (System > Tools > Updates > **[Import]** button). The system update file will load an update in both the EM7 Releases and the ScienceLogic OS section. You must wait until the update file has imported successfully (i.e. the **Import Status** column displays *Complete*) before importing the next update file.

- Import the 8.8.0 system update file in the System Updates page (System > Tools > Updates > **[Import]** button). The system update file will load an update in both the EM7 Releases and the ScienceLogic OS section. You must wait until the update file has imported successfully (i.e. the **Import Status** column displays *Complete*) before importing the next update file.

- Import the 8.9.0 system update file in the System Updates page (System > Tools > Updates > **[Import]** button). The system update file will load an update in both the EM7 Releases and the ScienceLogic OS section. You must wait until the update file has imported successfully (i.e. the **Import Status** column displays *Complete*) before importing the next update file.

- Import the 8.10.0 system update file in the System Updates page (System > Tools > Updates > **[Import]** button). The system update file will load an update in both the EM7 Releases and the ScienceLogic OS section. You must wait until the update file has imported successfully (i.e. the **Import Status** column displays *Complete*) before importing the next update file.

- Go to step #10 and continue.

6. *If you are currently running an 8.7 release*:

- From the ScienceLogic portal, download the 8.8.0,8.9.0, 8.10.0, and 8.10.1.3 updates to a local computer. Unzip any zipped files.

- Import the 8.8.0 system update file in the System Updates page (System > Tools > Updates > **[Import]** button). The system update file will load an update in both the EM7 Releases and the ScienceLogic OS section. You must wait until the update file has imported successfully (i.e. the **Import Status** column displays *Complete*) before importing the next update file.

- Import the 8.9.0 system update file in the System Updates page (System > Tools > Updates > **[Import]** button). The system update file will load an update in both the EM7 Releases and the ScienceLogic OS section. You must wait until the update file has imported successfully (i.e. the **Import Status** column displays *Complete*) before importing the next update file.

- Import the 8.10.0 system update file in the System Updates page (System > Tools > Updates > **[Import]** button). The system update file will load an update in both the EM7 Releases and the ScienceLogic OS section. You must wait until the update file has imported successfully (i.e. the **Import Status** column displays *Complete*) before importing the next update file.

- Continue to step #10.

7. *If you are currently running an 8.8 release*:

- From the ScienceLogic portal, download the 8.9.0, 8.10.0, and 8.10.1.3 updates to a local computer. Unzip any zipped files.

- Import the 8.9.0 system update file in the System Updates page (System > Tools > Updates > [Import] button). The system update file will load an update in both the EM7 Releases and the ScienceLogic OS section. You must wait until the update file has imported successfully (i.e. the *Import Status* column displays *Complete*) before importing the next update file.

- Import the 8.10.0 system update file in the System Updates page (System > Tools > Updates > [Import] button). The system update file will load an update in both the EM7 Releases and the ScienceLogic OS section. You must wait until the update file has imported successfully (i.e. the *Import Status* column displays *Complete*) before importing the next update file.

- Go to step #10 and continue.

8. *If you are currently running an 8.9 release*:

  - From the ScienceLogic portal, download the 8.10.0 and 8.10.1.3 update to a local computer. Unzip any zipped files.

  - Import the 8.10.0 system update file in the System Updates page (System > Tools > Updates > [Import] button). The system update file will load an update in both the EM7 Releases and the ScienceLogic OS section. You must wait until the update file has imported successfully (i.e. the *Import Status* column displays *Complete*) before importing the next update file.

  - Go to step #10 and continue.

9. *If you are currently running the 8.10.0 release*:

  - From the ScienceLogic portal, download the 8.10.1.3 update to a local computer. Unzip any zipped files.

  - Go to step #10 and continue.

10. Import the 8.10.1.3 system update file in the **System Updates** page (System > Tools > Updates > [Import] button).

  - The system update file will load an update named **EM7 8.10.1.3** in the EM7 Releases pane.

  - If you did have not installed 8.10.1, the system update file will load an update named **Platform 2018-12-04** in the ScienceLogic OS pane.

NOTE: In the ScienceLogic OS section, the **Deployment** column might display incorrect information for all rows except for the first row. If any row other than the first displays an incomplete count during the upgrade process, that incomplete count can be safely ignored.

---

11. After 8.10.1.3 has been imported:
  - Select the checkbox for the new update (EM7 8.10.1.3) in the EM7 Releases pane.
  - Select the checkbox for the new update (Platform 2018-12-04) in the ScienceLogic OS pane.

- In the **Select Action** menu, select *Stage Update (prepare for installation)*.
- The platform will stage the updates.

12. When staging has completed, install the update in the ScienceLogic OS pane (Platform 2018-12-04). To do so, select the lightning-bolt icon ( ) for the latest Platform update.

     The following warnings might appear; these warnings can be safely ignored:

     ```
     Package installation: warning: %postun(OpenIPMI-libs-2.0.19-11.el7.x86_64)
     scriptlet failed, exit status 1
     Package installation: warning: file /var/run/OpenIPMI: remove failed: No such
     file or directory
     ```

13. When staging has completed, install the 8.10.1.3 update in the EM7 Releases section. To do so, select the lightning-bolt icon ( ) for the update.

     The following warning might be generated; you can safely ignore this warning:

     ```
     502 Bad Gateway
     ```

     If you see this warning, reload the page in your browser.

14. Clear your browser's cache.

15. Clear the SL1 cache.
    - Go to the **Cache Management** page (System > Tools > Cache).
    - From the hamburger menu (☰), select **Clear EM7 System Cache**.

16. If you have not previously upgraded to 8.2.0, perform the steps listed in the *Other Manual Updates* section.

17. Go to the **PowerPack Manager** page (System > Manage > PowerPacks) and install all updated PowerPacks. Updated PowerPacks are loaded on your ScienceLogic system by the patch process. To install an updated PowerPack, find the PowerPack in the **PowerPack Manager** page and select the installation icon ( ) in the **Update** column for the PowerPack or use the *Update PowerPacks* option in the **Select Action** drop-down list.

> **TIP**: By default, installing an updated version of a PowerPack will overwrite all content in that PowerPack that has already been installed on the target system. You can use the **Enable Selective PowerPack Field Protection** setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields.

18. If you are monitoring devices using the ScienceLogic Agent, follow the steps listed in the **Agent Monitoring** manual to upgrade to the latest version of the Agent.

19. ***If you have not previously installed 8.10.1 and then rebooted all appliances, you must do so after installing 8.10.1.3.*** To reboot all appliances, perform the steps listed in the *Rebooting Appliances* section that are applicable to your system architecture. If you would like assistance in planning an upgrade path that meets your security needs while minimizing downtime, please contact your Customer Success Manager.

Upgrading MariaDB

Version 8.10.1 required updates to MariaDB that address security and performance issues. You can download the latest approved MariaDB updates at https://portal.sciencelogic.com/portal/miscellaneous.

NOTE: To address security issues, download the latest MariaDB updates. Earlier MariaDB updates remain on the portal to support users who have not yet migrated to the latest release.

The following sections describe how to perform this upgrade for different appliance types and architectures.

Two Database Servers Configured for High Availability

To upgrade a High Availability cluster, perform the following steps:

WARNING: The system will be unavailable when performing these steps.

1. Copy the MariaDB RPMs to the file system of both appliances.

2. Log in to the command-line of both Database Server appliances as em7admin.

3. Execute the following command on the secondary Database Server:

   ```
   sudo systemctl stop pacemaker.service
   ```

4. Execute the following command on the primary Database Server:

   ```
   sudo crm resource stop mysql
   ```

5. Execute the following command on the primary Database Server to determine the current installed version of the RPMs:

   ```
   sudo rpm -qa ^MariaDB-*
   ```

6. On the primary Database Server, navigate to the directory that you copied the RPMs.

7. For each RPM that the output from step 5 showed at an earlier version, execute the following command on the primary Database Server:

   ```
   sudo rpm -Uvh <file name of RPM>
   ```

8. Execute the following command on the primary Database Server to validate that the RPMs installed correctly:

   ```
   sudo rpm -qa ^MariaDB-*
   ```

9. Execute the following command on the primary Database Server:

   ```
   sudo crm resource start mysql
   ```

10. Execute the following command on the primary Database Server, replacing the password for the root database user where indicated:

```
            sudo mysql_upgrade -u root -p
```

11. On the secondary Database Server, execute the following command to determine the current installed version of the RPMs:

```
     sudo rpm -qa ^MariaDB-*
```

12. On the secondary Database Server, navigate to the directory where you copied the RPMs.

13. For each RPM that the output from step 11 showed at an earlier version of MariaDB, execute the following command on the secondary Database Server:

```
     sudo rpm -Uvh <file name of RPM>
```

14. Execute the following command on the secondary Database Server to validate that the RPMs installed correctly:

```
     sudo rpm -qa ^MariaDB-*
```

15. Execute the following command on the secondary Database Server:

```
     sudo systemctl start pacemaker.service
```

Two Database Servers Configured for Disaster Recovery

To upgrade two Database Servers configured for disaster recovery, perform the following steps:

> **WARNING:** The system will be unavailable when performing these steps.

1. Copy the latest RPMs to the file system of both appliances.
2. Log in to the command-line of both Database Server appliances as em7admin.
3. Execute the following command on the primary Database Server:

```
     sudo crm resource stop mysql
```

4. Execute the following command on the primary Database Server to determine the current installed version of the RPMs:

```
     sudo rpm -qa ^MariaDB-*
```

5. On the primary Database Server, navigate to the directory that you copied the RPMs.
6. For each RPM that the output from step 4 showed at an earlier version, execute the following command on the primary Database Server:

```
     sudo rpm -Uvh <file name of RPM>
```

7. Execute the following command on the primary Database Server to validate that the RPMs installed correctly:

```
     sudo rpm -qa ^MariaDB-*
```

8. Execute the following command on the primary Database Server:

```
     sudo crm resource start mysql
```

9. Execute the following command on the primary Database Server, replacing the password for the root database user where indicated:

```
sudo mysql_upgrade -u root -p
```

10. On the secondary Database Server, execute the following command to determine the current installed version of the RPMs:

```
sudo rpm -qa ^MariaDB-*
```

11. On the secondary Database Server, navigate to the directory where you copied the RPMs.

12. For each RPM that the output from step 10 showed at an earlier version, execute the following command on the secondary Database Server:

```
sudo rpm -Uvh <file name of RPM>
```

13. Execute the following command on the secondary Database Server to validate that the RPMs installed correctly:

```
sudo rpm -qa ^MariaDB-*
```

Three Database Servers Configured for HA and DR

To upgrade a High Availability cluster, perform the following steps:

WARNING: The system will be unavailable when performing these steps.

1. Copy the latest RPMs to the file system of all three appliances.
2. Log in to the command-line of all three Database Server appliances as em7admin.
3. Execute the following command on the secondary Database Server in the HA cluster:

```
sudo systemctl stop pacemaker.service
```

4. Execute the following command on the primary Database Server in the HA cluster:

```
sudo crm resource stop mysql
```

5. Execute the following command on the primary Database Server in the HA cluster to determine the current installed version of the RPMs:

```
sudo rpm -qa ^MariaDB-*
```

6. On the primary Database Server in the HA cluster, navigate to the directory that you copied the RPMs.
7. For each RPM that the output from step 5 showed at an earlier version, execute the following command on the primary Database Server in the HA cluster:

```
sudo rpm -Uvh <file name of RPM>
```

8. Execute the following command on the primary Database Server in the HA cluster to validate that the RPMs installed correctly:

```
sudo rpm -qa ^MariaDB-*
```

9. Execute the following command on the primary Database Server in the HA cluster:

```
            sudo crm resource start mysql
```

10. Execute the following command on the primary Database Server in the HA cluster, replacing the password for the root database user where indicated:

```
sudo mysql_upgrade -u root -p
```

11. On the secondary Database Server, execute the following command to determine the current installed version of the RPMs:

```
sudo rpm -qa ^MariaDB-*
```

12. On the secondary Database Server, navigate to the directory where you copied the RPMs.

13. For each RPM that the output from step 11 showed at an earlier version, execute the following command on the secondary Database Server:

```
sudo rpm -Uvh <file name of RPM>
```

14. Execute the following command on the secondary Database Server in the HA cluster to validate that the RPMs installed correctly:

```
sudo rpm -qa ^MariaDB-*
```

15. Execute the following command on the secondary Database Server in the HA cluster:

```
sudo systemctl start pacemaker.service
```

16. On the Database Server for disaster recovery, execute the following command to determine the current installed version of the RPMs:

```
sudo rpm -qa ^MariaDB-*
```

17. On the Database Server for disaster recovery, navigate to the directory that you copied the RPMs.

18. For each RPM that the output from step 16 showed at an earlier version, execute the following command on the Database Server for disaster recovery:

```
sudo rpm -Uvh <file name of RPM>
```

19. Execute the following command on the secondary Database Server in the HA cluster to validate that the RPMs installed correctly:

```
sudo rpm -qa ^MariaDB-*
```

20. Execute the following command on the Database Server for disaster recovery to validate that the RPMs installed correctly:

```
sudo rpm -qa ^MariaDB-*
```

Single Database Server/All-In-One Appliance/Data Collector/Message Collector

To upgrade MariaDB on a single Database Server, All-In-One Appliance, Data Collector, or Message Collector, perform the following steps:

> **WARNING:** The Database Server, All-In-One Appliance, Data Collector, or Message Collector will be
> inoperable when performing these steps.

1. Copy the latest RPMs to the file system of the appliance:

2. Log in to the command-line of the appliance as em7admin.

3. Execute the following commands:

   ```
   sudo systemctl stop em7
   sudo systemctl stop mariadb.service
   ```

4. Execute the following command to determine the current installed version of the RPMs:

   ```
   sudo rpm -qa ^MariaDB-*
   ```

5. Navigate to the directory that you copied the RPMs.

6. For each RPM that the output from step 4 showed at an earlier version, execute the following command:

   ```
   sudo rpm -Uvh <file name of RPM>
   ```

7. Execute the following command to validate that the RPMs installed correctly:

   ```
   sudo rpm -qa ^MariaDB-*
   ```

8. Execute the following commands:

   ```
   sudo systemctl daemon-reload
   sudo systemctl start mariadb.service
   sudo systemctl start em7
   ```

9. Execute the following command, replacing the password for the root database user where indicated:

   ```
   sudo mysql_upgrade -u root -p
   ```

Manual Updates for 8.1.x Systems Updated to 8.10.1.3

If you upgraded from an 8.1.x system to 8.10.1.3, after 8.10.1.3 is installed, you must manually apply the
following changes to every Message Collector and All-In-One Appliance in your system:

1. Either go to the console or use SSH to access the server.

2. Log in as user **em7admin** with the appropriate password.

3. Enter the following at the command line:

   ```
   sudo vi /etc/siteconfig/siloconf.siteconfig
   ```

4. Locate the following line:

   ```
   eventmanager = syslog,trap,internal
   ```

> **NOTE:** On an All-In-One Appliance, this line will include additional entries in the comma-delimited list.

5. Add ",agent" to the end of the line. The line should now look like this:

```
eventmanager = syslog,trap,internal,agent
```

6. Save the file and exit vi (:wq).

7. At the command line, enter the following command to rebuild the configuration file:

```
sudo /opt/em7/share/scripts/generate-silo-conf.py > /etc/silo.conf
```

Rebooting Appliances

Use the applicable steps listed in this section to reboot your appliances.

Administration Portal

Perform the following steps to reboot an Administration Portal:

1. Either go to the console of the Database Server or use SSH to access the server.

2. Log in as *em7admin* with the appropriate password.

3. At the shell prompt, execute the following:

```
python -m silo_common.admin_toolbox <appliance_ID> "/usr/bin/sudo /usr/sbin/shutdown -r +1"
```

    where:

- *appliance_ID* is the appliance ID for the Data Collector, Message Collector, or Administration Portal.

If your SL1 system includes multiple Administration Portals, you can remotely reboot the Administration Portals from an Administration Portal. To do so:

1. Go to the **Appliance Manager** page (System > Settings > Appliances).

2. Select the checkboxes for the appliances you want to reboot.

3. In the **[Select Action]** menu, select *Reboot* and click the Go button.

4. Click the OK button when the "Are you sure you want to reboot the selected appliances?" message is displayed.

5. During the reboot, the user interface for the affected Administration Portals is unavailable.

6. When the reboot has completed, the **Audit Logs** page (System > Monitor > Audit Logs) will include an entry for each appliance that was rebooted.

Data Collectors and Message Collectors

You can reboot Data Collector and Message Collectors either from the user interface or from the command line.

From the SL1 user interface, perform the following steps to reboot a Data Collector or Message Collector:

1. Go to the **Appliance Manager** page (System > Settings > Appliances).

2. Select the checkboxes for the appliances you want to reboot.

3. In the **[Select Action]** menu, select *Reboot* and click the Go button.

4. Click the OK button when the "Are you sure you want to reboot the selected appliances?" message is displayed.

5. During the reboot, go to the **System Logs** page (System > Monitor > System Logs). You should see this message:

   ```
   Major: Could not connect to module (5) database USING SSL=TRUE: Error attempting
   to connect to database with SSL enabled True: (2003, 'Can't connect to MySQL
   server on '10.2.12.77' (113 "No route to host")')
   ```

6. When the reboot has completed, the **Audit Logs** page (System > Monitor > Audit Logs) will include an entry for each appliance that was rebooted.

From the console of the Database Server or SSH to the Database Server, perform the following steps to reboot a Data Collector or Message Collector:

1. Either go to the console of a Database Server or SSH to access the server.

2. Log in as *em7admin* with the appropriate password.

3. At the shell prompt, execute the following:

   ```
   python -m silo_common.admin_toolbox <appliance_ID> "/usr/bin/sudo /usr/sbin/shutdown
   -r +1"
   ```

   where:

   - *appliance_ID* is the appliance ID for the Data Collector, Message Collector, or Administration Portal.

Standalone All-In-One Appliances and Database Servers

Perform the following steps to reboot a standalone All-In-One Appliance or Database Server:

1. Either go to the console or use SSH to access the server.

2. Log in as *em7admin* with the appropriate password.

3. Execute the following commands on the appliance to pause the system and shutdown MariaDB. Enter the password for the em7admin user when prompted:
   ```
   sudo touch /tmp/.proc_mgr_pause
   sudo systemctl stop mariadb
   ```

4. Execute the following command on the appliance to reboot the appliance:

```
sudo reboot
```

5. After the appliance has rebooted, log in to the appliance as the em7admin user using the console or SSH.

6. Execute the following command on the appliance to un-pause the system:

```
sudo rm /tmp/.proc_mgr_pause
```

7. Enter the password for the em7admin user and confirm the command when prompted.

Two Database Servers Configured for Disaster Recovery

Perform the following steps to reboot two Database Servers configured for Disaster Recovery:

1. Either go to the console of the primary Database Server or use SSH to access the server.

2. Log in as **em7admin** with the appropriate password.

3. First, you should check the status of the appliances. To do this, enter the following at the shell prompt:

```
cat /proc/drbd
```

4. Your output will look like this:

```
1: cs:Connected ro:Primary/Secondary ds:UpToDate/UpToDate C r----
ns:17567744 al:0 bm:1072 lo:0 pe:0 ua:0 ap:0 ep:1 wo:b oos:12521012
```

> **NOTE:** If your output includes "ro:Primary/Secondary", but does not include "UpToDate/UpToDate", data is being synchronized between the two appliances. You must wait until data synchronization has finished before rebooting.

5. Execute the following commands on the **primary** appliance to pause the system and shutdown MariaDB. Enter the password for the em7admin user when prompted:

```
sudo touch /tmp/.proc_mgr_pause
sudo systemctl stop pacemaker
```

6. Execute the following command on the **primary** appliance to reboot the appliance:

```
sudo reboot
```

7. After the primary appliance has rebooted, log in to the console of the **primary** appliance again.

8. Execute the following commands on the **primary** appliance:

```
sudo rm /tmp/.proc_mgr_pause
```

9. Enter the password for the em7admin user and confirm the command when prompted.

10. Log in to the **secondary** Database Server as the em7admin user using the console or SSH.

11. Execute the following command on the **secondary** appliance to reboot the appliance:

```
sudo reboot
```

12. Enter the password for the em7admin user when prompted.

Two Database Servers in a High Availability Cluster

Perform the following steps to reboot two Database Servers in a high availability cluster:

1. Either go to the console of the secondary Database Server or use SSH to access the server.

2. Log in as **em7admin** with the appropriate password.

3. First, you should check the status of the appliances. To do this, enter the following at the shell prompt:

    ```
    cat /proc/drbd
    ```

4. Your output will look like this:

    ```
    1: cs:Connected ro:Secondary/Primary ds:UpToDate/UpToDate C r----
    ns:17567744 al:0 bm:1072 lo:0 pe:0 ua:0 ap:0 ep:1 wo:b oos:12521012
    ```

NOTE: If your output includes "ro:Secondary/Primary", but does not include "UpToDate/UpToDate", data is being synchronized between the two appliances. You must wait until data synchronization has finished before rebooting.

5. Execute the following command on the **secondary** appliance to stop the cluster service:

    ```
    sudo systemctl stop pacemaker
    ```

6. Enter the password for the em7admin user when prompted.

7. Log in to the **primary** Database Server as the em7admin user using the console or SSH.

8. Execute the following commands on the **primary** appliance to pause the system and stop the cluster service. Enter the password for the em7admin user when prompted:

    ```
    sudo touch /tmp/.proc_mgr_pause
    sudo systemctl stop pacemaker
    ```

9. Execute the following command on the **primary** appliance to reboot the appliance:

    ```
    sudo reboot
    ```

10. After the primary appliance has rebooted, log in to the console of the **primary** appliance again.

11. Execute the following command on the **primary** appliance:

    ```
    sudo rm /tmp/.proc_mgr_pause
    ```

12. Enter the password for the em7admin user and confirm the command when prompted.

13. Ensure that the user interface is now available on the primary appliance.

14. Log in to the **secondary** Database Server as the em7admin user using the console or SSH.

15. Execute the following command on the **secondary** appliance to reboot the appliance:

    ```
    sudo reboot
    ```

16. Enter the password for the em7admin user when prompted.

Three Database Servers Configured for High Availability and Disaster Recovery

Perform the following steps to reboot three Database Servers configured for high availability and disaster recovery:

1. Either go to the console of the **secondary Database Server in the HA cluster** or use SSH to access the server.

2. Log in as *em7admin* with the appropriate password.

3. First, you should check the status of the appliances. To do this, enter the following at the shell prompt:

    ```
    cat /proc/drbd
    ```

4. Your output will look like this:

    ```
    10: cs:Connected ro:Secondary/Primary ds:UpToDate/UpToDate C r----
    ns:17567744 al:0 bm:1072 lo:0 pe:0 ua:0 ap:0 ep:1 wo:b oos:12521012
    ```

> **NOTE**: If your output includes "ro:Secondary/Primary", but does not include "UpToDate/UpToDate", data is being synchronized between the two appliances. You must wait until data synchronization has finished before rebooting.

5. Execute the following command on the **secondary Database Server in the HA cluster** to stop the cluster service:

    ```
    sudo systemctl stop pacemaker
    ```

6. Enter the password for the em7admin user when prompted.

7. Log in to **primary** Database Server as the em7admin user using the console or SSH.

8. Execute the following commands on the **primary** appliance to pause the system and stop the cluster service. Enter the password for the em7admin user when prompted:

    ```
    sudo touch /tmp/.proc_mgr_pause
    sudo systemctl stop pacemaker
    ```

9. Execute the following command on the **primary** appliance to reboot the appliance:

    ```
    sudo reboot
    ```

10. After the primary appliance has rebooted, log in to the console of the **primary** appliance again.

11. Execute the following command on the **primary** appliance:

    ```
    sudo rm /tmp/.proc_mgr_pause
    ```

12. Enter the password for the em7admin user and confirm the command when prompted.

13. Log in to the **secondary Database Server in the HA cluster** as the em7admin user using the console or SSH.

14. Execute the following command on the **secondary Database Server in the HA cluster** to reboot the appliance:

    ```
    sudo reboot
    ```

15. Enter the password for the em7admin user when prompted.

16. Log in to the **Database Server for Disaster Recovery** as the em7admin user using the console or SSH.

17. Execute the following command on the **Database Server for Disaster Recovery** to reboot the appliance:

    ```
    sudo reboot
    ```

18. Enter the password for the em7admin user when prompted.

Deprecated Features

As of the 8.2.0 release, the following PowerPacks are no longer included in the default ISO. These PowerPacks will not be automatically removed from an existing system during an upgrade and will remain available for download on the [ScienceLogic Portal](#):

- ADIC Base Pack
- Ascend Communications Base Pack
- Cabletron System Base Pack
- CloudKick Management
- GoGrid Base Pack
- Informant Cluster
- Informant Exchange
- Informant MS SQL
- Informant Windows OS
- NTI Base Pack
- Rackspace Base Pack
- Redback Base Pack
- RIM Blackberry Base Pack
- Sensatronics Base Pack
- SystemEdge Base Pack
- System Uptime
- Tipping Point Base Pack
- Xirrus Base Pack

The new user interface architecture requires API access for all users; API access is automatically granted to users. The following API-specific access hooks have been deprecated and removed from the product:

- API: Resource Indexes
- API: Server Access
- API: Virtual Device

The following functionality that was available in previous releases is no longer available in the 8.10.1.3 release:

- The process for generating rollup/normalized data has been updated to improve performance and scalability. This update deprecates the generation of frequent rollup data. The following user interface pages are affected:
  - The widgets Leaderboard/Top-N, Leaderboard/Top-N (secondary), and Multi-Series Performance no longer support Frequent normalization. If these widgets are used by older dashboards and are already configured to use Frequent normalization, the platform will automatically update these widgets to use hourly normalization.
  - In the Collection Labels page (System > Manage > Collection Labels), the Frequent Data column is deprecated.
- The Cisco Nexus PowerPack has been removed from the default build and is no longer supported. However, the PowerPack is not deleted during the upgrade process. The device classes for Cisco Nexus devices are now included in the Cisco: Base Pack PowerPack.
- The ScienceLogic Agent no longer supports 32-bit versions of Linux or Windows.
- The third-party Azure python library has been removed from the ISO build.
- The FTP, SFTP, NFS, and SMB backup options that stage locally are no longer supported.
- The EMC Base Pack PowerPack has been removed from the default build and is no longer supported. However, the PowerPack is not deleted during the upgrade process. If you are still using the EMC Base Pack PowerPack, ScienceLogic recommends using the EMC: VNX PowerPack instead.
- The SAN wizard is no longer supported. ScienceLogic will no longer provide direct support for configuring a SAN for data storage.
- Integration Server appliances are no longer supported.
- Root access is not enabled on any appliance.
- The VMware: vCloud PowerPack has been removed from the ISO build and is no longer supported.
- The "ifconfig" command is no longer supported by the new appliance operating system. The "ip addr" command must be used instead.
- NOC Screens (System > Manage > Screens) are no longer included in the platform. To re-enable this feature, contact ScienceLogic Customer Support.
- The Knowledge Base is no longer supported by ScienceLogic and will be disabled by default for new users.

Known Issues

Agent Monitoring

- Agent monitoring does not work if the Agent installation is performed for an already discovered device using an organization setting that is different from the current organization for the device.

- Log File Monitoring Policies do not work if the policy is applied before the log file is created.

- A Windows 7 server discovered by an Agent is incorrectly categorized as a Windows 2012 Server.

- The AWS t2.nano instances have severe memory constraints. For this reason, the Agent for Linux will run only on t2.micro or larger devices.

API

- API calls for Interface Packet performance data runs an unnecessary SQL query for CBQoS tables, creating unnecessary overhead.

- API calls to IFP normalized performance data cannot filter on the metric value and return a null value.

- API calls to CBQoS normalized performance data cannot filter on the metric value and return a null value.

AWS AMI

- In 8.5.x and 8.6.0 an intermittent issue prevents users from accessing the user interface for Database Servers built from the AWS AMI.

  - *Workaround:* Go to the console of the Database Server or log in using SSH. Execute the following commands at the shell prompt:

    ```
    cd /etc/nginx/
    openssl req -x509 -sha256 -nodes -days 365 -newkey rsa:2048 -keyout
    silossl.key -out silossl.pem
    systemctl start nginx
    systemctl status nginx
    ```

Backups

- The size of the default partition for local configuration backups is not suitable for most systems. If you require local configuration backups, contact ScienceLogic Customer Support for assistance with utilizing a larger partition.

CBQoS

- In the Device Performance page, the Navigation Bar displays CBQoS entries with the name "Overview (%)", but the user is unable to generate these reports using raw data. The user can generate these reports using normalized data. The user can generate all other CBQoS device performance reports, including reports for "Overview (<unit>)".

- If you discover a CBQoS device but don't enable any CBQoS collection for any interface on that device, the platform will attempt collection of CBQoS statistics and will generate entries in the silo_query.log

- Under high-load conditions, an unhandled exception might occur when CBQoS collection starts collecting data from a device.

Configuration Dynamic Applications

- In 8.10.1, addressed an issue with the PowerPacks "Windows Restart Automatic Services" and "Microsoft: Windows Server Services". The Dynamic Applications "Windows Find Automatic Services Not Running" and "Microsoft: Windows Server Service Configuration" were generating unhandled exceptions. Although 8.10.1 includes a fix for this problem, some users might not see collected configuration data after patching up to 8.10.1.

  > To workaround this problem, for each device associated with these Dynamic applications, go to the console or SSH to the Data Collector associated with the Dynamic Applications and run the following SQL command:
  >
  > At the shell prompt, enter silo_mysql to get an sql prompt. Then run the following command:
  >
  > ```
  > DELETE FROM collector_state.config_last_poll where did = <device_id> and app_
  > id IN (<dynamic_application_id_1><dynamic_application_id_2>)
  > ```
  >
  > where:

  - <device_id> is the device for which you want to view configuration data collected by the two Dynamic Applications.
  - <dynamic_application_id_1,<dynamic_application_id_2> are the IDs associated with the two Dynamic Applications.

Data Collectors

- When a Data Collector is built with the 8.5.0 release, added to a distributed system that is built with 8.5.1.2, and device discovery begins, the system log includes an unhandled exception related to the Data Collector. When the Data Collector is updated to 8.5.1.2, the issue is resolved.

Dashboards

- Exporting dashboard widgets to PDF does not work.
- The Custom Table widget does not read context correctly if one or more rows are selected.

Device Performance

- When generating reports in CSV format in the Device Performance page (select report > **[Report]** button > **CSV**), the exported report displays some values in the incorrect columns.

Device Vanish/Device Purge

- If users set the **Component Vanish Timeout** field to "0" (zero) in the **System Thresholds Default** page (System > Settings > Thresholds > System), component devices should never be set to "vanish" mode. If users also set the **Component Purge Timeout** to any value other than zero in the **System Thresholds Default** page (System > Settings > Thresholds > System), component devices will be purged without ever being set to "vanish" mode. To prevent this behavior, set both **Component Vanish Timeout** and **Component Purge** Timeout to "0" (zero).

EMC

- The "EMC: VNX Enclosure Configuration" Dynamic Application is failing to collect data for Chassis Name, Chassis Type, Health State, Operational Description, Operational Status, Average Air Temperature, Current Air Temperature, Average Input Power, and Current Input Power.

Events

- If users select an event that was trigged by data collected with the ScienceLogic Agent, the link to the incident that triggered the event (usr/local/silo/gui/ap/www/responder-ui/incident/4/index.em7) is broken.

IT Services

- The Select IT Service Owner modal page does not display any users.

Microsoft: SQL Enhanced

- On 8.6.0, when the Data Collector is over-burdened or the monitored Windows system is slow, one or more Dynamic applications in the Microsoft: SQL Enhanced PowerPack can sigterm.

phpMyAdmin

- phpMyAdmin fails to connect to the database on Data Collection servers or Message Collection servers and displays error message "#1045 - Access denied for user 'root'".

    - *Workaround*. Go to the console of the Database Server or log in using SSH. Edit the following file:
    - /etc/siteconfig/siloconf.siteconfig1
    - Remove the lines for ap_user and ap_pass.

Platform

- When changing the IP address of a Data Collector or a Message Collector, the platform will generate an unhandled exception until the IP address is changed in the System > Settings > Appliances page.

SoftLayer

- After installing the PowerPack "SoftLayer: Cloud" and discovering a Bare Metal Server, the Device Performance report for "Public Network Performance Dynamic Application > Public Network Throughput" displays incorrect values.

Standard Deviation

- There is a relationship between the value in the *min weeks data* field (for standard deviation objects) in the

    Collections Objects page (System > Manage > Applications > wrench icon > Collections) and the value in *Raw Data Retention* in the **Device Thresholds** page (Registry > Devices > Device Manager > wrench icon > Thresholds) for a Data Collector or the global value in the *Raw Performance Data* field in the **Data Retention Settings** page (System > Settings > Data Retention). Note that the threshold defined for the device overrides the global threshold defined in the **Data Retention Settings** page. If the value in the *min weeks data* field.

Updates/Installation

- In the System Updates page (System > Tools > Updates), older ScienceLogic OS appears, with lightning-bolt icon ( ) after the latest version of the ScienceLogic OS is successfully deployed.

- In the System Updates page (System > Tools > Updates), in some situations, the *Deployment* column in the **ScienceLogic OS** pane mistakenly displays a partial update. If you select the log icon ( ), the log shows that all appliances were updated.

- The appliance selection screen that appears during the installation erroneously lists the deprecated Integration Server appliance.

- An unhandled exception is generated when staging cannot complete.

- For users who use self-signed SSL certificates, when updating to 8.10.1. and later, you will see the spurious error message "Waiting for web server to respond". To clear the error message, refresh the page. This message does not affect the update. The refresh causes the browser to upload the newly generated, self-signed certificate to the server.

User Interface

- The System Logs page will fail to load when the number of available pages is approximately 400,000. As a workaround, you can select a higher page result count preference to decrease the number of pages.

- The lightning-bolt icon does not appear in the Monitors tab of the Device Administration panel.