ScienceLogic

SL1 Hollywood 12.2.3 Release Notes

SL1 version 12.2.3 (Document revision 3)

SL1 Hollywood 12.2.3 Release Notes

IMPORTANT: ScienceLogic strongly recommends that you review the ***upgrade instructions***, important notes about ***upgrading*** SL1, and ***known issues*** for this release before upgrading to SL1 12.2.3.

WARNING: SL1 no longer supports the legacy version of Data Pull. If you are upgrading from a version of SL1 prior to 12.2.1.2, you will need to update all of your SL1 appliances to version 12.2.3, including your Data Collectors and Message Collectors, to avoid potential data loss. When all appliances are successfully upgraded to 12.2.3, SL1 will automatically deprecate legacy Data Pull. If you do not update SL1 appliances after 60 days, the data on those appliances will be lost, and you will need to redeploy the appliances. For version 12.2.3, there is an issue that prevents data pull from properly deprecating older versions; for more information, see the following Knowledge Base article: https://support.sciencelogic.com/s/article/15573. This issue will be addressed in version 12.2.4 and is not present in version 12.3.0.

These release notes provide a comprehensive list of the features, enhancements, and addressed issues that are included in the SL1 Hollywood 12.2.3 release.

To view the updates that are included in previous SL1 Hollywood releases, see the following release notes:

- *12.2.0*
- *12.2.1.1*
- *12.2.1.2*

NOTE: Some of the features, enhancements, and addressed issues that are included in this SL1 platform release were originally included in the following SL1 AP2 releases:

- *8.7.37 (Espresso)*
- *8.7.96 (French Toast)*
- *8.14.26 (Gelato)*

AP2 version 8.14.26 (Gelato) is installed by default in SL1 12.2.3.

This document covers the following topics:

Before You Proceed

If you are planning to consume SL1 Hollywood 12.2.3, be advised of the following:

- This release is available only as a patch; there is no ISO version.
- STIG-compliant users cannot upgrade to this release.
- AWS deployments that are using Aurora 3 cannot upgrade to this release.
- You must currently be on a version of SL1 with all appliances running on Oracle Linux 8 (OL8) before you can upgrade to this release.
- You can upgrade to this release directly from SL1 12.2.1.1 or 12.2.1.2.

For more details about these items and other potential issues you might experience, see the *Important Upgrade Notes* and *Known Issues* sections.

New Features and Enhancements in SL1 Hollywood 12.2.3

Anomaly Detection

- Added the new **Skylar AI** page to the left-hand navigation and the **Advanced Menu** page. Currently, the **Skylar AI** page does not contain any content, but future AP2 releases will add links and other information to this page.
- The **Machine Learning** page was renamed **Anomaly Detection**, and the **Machine Learning Thresholds** page was renamed **Anomaly Detection Thresholds**.
- The URLs in SL1 for the **Anomaly Detection** and **Anomaly Detection Thresholds** pages were updated from **/aiml** to the following structure: **/skylar-ai/anomaly-detection** and **/skylar-ai/anomaly-detection/thresholds**.

> **NOTE:** To access the **Anomaly Detection** page and the **Anomaly Detection Thresholds** page, add "skylar-ai/anomaly-detection" or "skylar-ai/anomaly-detection/thresholds" to the URL for your SL1 system. For example: https://sl1.com/skylar-ai/anomaly-detection. Currently, these pages do not display in the left-hand navigation under the Skylar AI icon.

- The **Anomaly Detection** page (formerly the **Machine Learning** page) now lists every Dynamic Application metric with its Anomaly Detection status, even metrics that will not alert when the anomaly score exceeds a threshold.
- For an SL1 system that is connected to a Skylar Automated RCA system, the ***Anomaly Detection*** column was removed from the **Anomaly Detection** page, as this column is no longer relevant with this release. Any devices listed on the **Anomaly Detection** page have anomaly detection enabled by default. This column was also removed from the **Device Investigator**, **Event Investigator**, and **Service Investigator** pages that contain anomaly detection data.
- The Skylar AI logo in the main navigation menu now adjusts its color based on the theme you are currently on (light vs dark).

Business Services

- The **Business Services** and **Service Investigator** pages have been updated to include new features such as new information in the **Timeline** panel on the **Service Investigator** page. The following updates were made to support this enhancement:
    - Updated the Zebrium icon to the Skylar AI icon in the **Timeline** panel of the **Service Investigator** page.
    - The **Timeline** panel now shows the health, availability, and risk statuses of your events in the last 7 days by default.
    - The ***Last Edited*** field in the **Overview** panel at the top of the **Service Investigator** page now displays the date the service was last edited.
    - You can now enable or disable services in bulk on the **Business Services** page.
    - Added a ***Refresh Interval*** column to the **Business Services** page. This field, also known as the polling frequency, is the frequency at which data is communicated between a device and another system.
- The **Policies** page was renamed the **Service Policies** page, and the following columns were added to the page:
    - ***Status***: The status of the service policy. This field indicates if the service policy you have selected is "Valid" or "Invalid".
    - ***Service Count***: The number of services assigned to the policy.
    - ***Date Edited***: The date the service policy was last edited.
    - ***Last Edited By***: The user to last edit the service policy.
- Updated the default Business Services policy so that device availability reflects the active status of constituent devices for physical and component devices. The following updates were made to support this enhancement:
    - Replaced availability vital metrics and the "All Devices" filter with "isActive=True".
    - Replaced the aggregation type of "Availability" with "Count".
    - Set the rule to "Available" if at least one device has the "IsActive=True" filter.
    - Updated the default aggregation factor for IT, Business, and Services Model service policies from "Average" to "Minimum".
- The **Business Services** page now uses a new GraphQL query that collects metric anomalies for your devices.
- Updated the status policies for "Aggregate," "Business," and "IT" services and their corresponding rules for calculating health, availability, and risk values.
- The onDemand process now retrieves data by calculating the "lastValue" in the last three intervals. If the value of the two most recent intervals is null, the system will log the calculation as incomplete because metrics did not exist during that time.

Credentials

- SL1 12.2.3 includes package updates to the Enterprise Key Management Service (EKMS) to improve security and performance.

Dashboards

- The widgets on the **Dashboards** page can now display different scale prefix options for non-percentage-based metrics. You can select one of these scale prefixes, such as Kilo, Mega, Giga, and Tera, if you want dashboards to auto-scale the visualization of metrics that have the same metric unit prefix.

  To do so, select the ***Scale prefix*** drop-down field in the ***Metrics & Properties*** column of the **Edit Widget** page, then select a unit of measurement to use from the drop-down field.

  The following updates were made to support this enhancement:

  - The widgets that use the following visualizations allow you to select different scale prefix options for non-percentage-based metrics:

    - Bar Chart
    - Table
    - Line Chart
    - Number
    - Leaderboard
    - Leaderboard Bar Chart
    - Forecast

  - The ***Select Visualization*** drop-down list on the **Create Widget** page now lists the available visualization options in alphabetical order.

- Added navigation to the **Device Dashboards** page (System > Customize > Device Dashboards) in the classic SL1 user interface.
- Removed the 50-return limit for ***Interface*** widgets with the *Table* visualization and added infinite scroll.
- Updated and organized information in the footer of tables, such as the total, selected, and filtered counts.

Device Management

- Added a new **Relationships and Memberships** panel to the **Device Investigator** page. This new panel displays details about the other devices and services that have relationships to the selected device.
- You can now edit **Device Investigator** layouts, copy layouts, and save existing layouts with different names.
- On the **Device Investigator**, the **[Machine Learning]** tab was renamed **[Anomaly Detection]**.

- Updated the method for performing bulk actions to multiple devices on the **Devices** page. Previously, you could select from several action-specific icons at the top of the page. With this update, those icons have been replaced by an ***Actions*** drop-down menu that includes a list of available bulk actions. In addition, that drop-down menu now includes a new *Schedule Maintenance* option for scheduling maintenance events on multiple selected devices.
- Updated the method for performing bulk actions to multiple devices on the **Devices** page. Previously, you could select from several action-specific icons at the top of the page. With this update, those icons have been replaced by an **[Actions]** drop-down menu that includes a list of available bulk actions, which now includes new options for scheduling maintenance events for devices, changing the collector group assigned to devices, and enabling or disabling data collection on devices.
- When deleting one or more devices that have associated asset records, you now have the option to delete the associated assets at the same time.
- In the Basic Menu and Advanced Menu, the **Device Manager** option was relabeled to **Classic Devices**.

Discovery

- When adding devices using the guided discovery process from the **Discovery Sessions** page (Devices > Discovery Sessions), devices for which your SL1 system does not have the required entities will now appear in a secondary section at the bottom with a new warning note. This note will specify why you cannot add the selected device and the necessary prerequisites.

Events

- Added a new **Skylar Analytics Summary** panel to the **Event Investigator** page for predictive alerts from Skylar AI. Predictive alerts work like events in SL1, except they are forecasting when a future event could happen, instead of reporting on an event that already occurred. The **Skylar Analytics Summary** panel displays a graph of data from Skylar AI that corresponds with the event ID.
- Added *Skyler AI* to the ***Event Source*** drop-down option. You can also filter your search by events sourced by Skylar AI on the event-related pages.
- On the **Event Policy Editor** page, the ***Skylar AI Severity*** drop-down for *Skylar AI* sourced events now defaults to *Disregard Severity*.
- A new *Table Preferences* menu is now available from the **Grid Settings** menu on the **Events** page.
- Replaced the text editor on the **Event Policy Editor** page with a front-end HTML editor for enabling text-editing capabilities for web applications and related software.
- Removed the "experimental" labels from several GraphQL resources that are now standard fields.
- Updated the error messages in the **[Suppression]** tab on the **Event Policies** page for policies with invalid device IDs.

Global Manager

- Changing the name of your Global Manager stack will retrieve and return the correct version information.

GraphQL

- Removed both the "enabled" and "status" fields from "aiMachineLearningMetricAnomalies" device queries in GraphQL and added an "alerting" status. The "alerting" status will send an alert whenever the anomaly score exceeds a set threshold, and then send an alert that maps to an event of the appropriate severity.
- Added a "deviceGroup" search parameter to the "relatedNodes" query in GraphQL to support the ***Relationships and Memberships*** panel in the **Device Investigator**.
- Updated the "deviceMetrics" query by adding new endpoints that enable any monitor-related data to be queried as a new "collectionType" object.
- Added the ability to search Dynamic Applications associated with specific presentation IDs by adding "presentationID" as an "IDSearch" variable for the existing "DynamicApplicationSearch" function. This update enables you to search Dynamic Applications by finding the corresponding APIs associated with specific presentation IDs.
- Added a new status variable to the GQL API for device groups. This variable represents the device statuses within a device group as a singular unit.
- When you run a GraphQL query for an "Appliance" type, you will also get the current operating system version for that appliance.
- Added a read-only, searchable "powerpackId" field to the "guidedDiscoveryWorkflow(s)" queries. This field displays the PowerPack ID. If the guided discovery workflow contains a reference to a PowerPack that is not installed on the system, it will return a placeholder object with its "powerpackId", a "name" that will display as "N/A", and an "id" of "-1".

Logging

- Audit logging was enhanced to include session ID renewal events.

Platform and Security

- SL1 version 12.2.3 includes multiple package updates to improve security and system performance.
- When logging in for the first time with a new SL1 user account, a **Notice** dialog appears, prompting you to accept an agreement that you may use the product only in accordance with the applicable contract and within the scope of the rights purchased by your organization. To accept, check the box and then click **[Agree]**.

System Updates

- Updated SL1 to enable upgrading MariaDB from the 10.4 line to the 10.6 line.
- Updated the `vimysql` command to handle configuration changes for MariaDB 10.6. The `vimysql` command automatically removes deprecated options from the configuration upon saving.
- When upgrading MariaDB, the "module_upgrade_mariadb" script that was previously used has been deprecated. With this release, users should now use the command "siloupdate upgrade-mariadb" to upgrade MariaDB packages on appliances in your SL1 stack.

- Upgrades to the MariaDB server and client package are now handled in a single transaction during the MariaDB upgrade phase. The client package is no longer upgraded during the system update on most SL1 appliance types, with the exception of Administration Portals and Data Engines.

User Interface

- Added a footer to the user interface that includes the current SL1 version and build number. Optionally, if you have selected the ***Display Previous Login In Footer*** checkbox on the **Behavior Settings** page (System > Settings > Behavior), this footer can also display the time stamp of your last successful or failed login attempt.
- Throughout SL1, references to "Zebrium" have been changed to "Skylar AI".
- Throughout SL1, references to "Machine Learning" and "Metric Anomalies" have both been changed to "Anomaly Detection".

Issues Addressed in SL1 Hollywood 12.2.3

Agent

- Addressed an issue that was causing calls to the agent endpoint to fail during collection in Gen 1 SL1 agents. (Case: 00390933) (Jira ID: EM-62213)

Asset Management

- Asset values from collection objects with a larger asset precedence setting will now be honored during Dynamic Application collection. (Case: 00452509) (Jira ID: EM-66153)

Authentication

- Updated authentication for the default user interface (AP2) to ensure that passwords that contain a colon character authenticate correctly, as they already did in the classic user interface. (Cases: 00271595, 00298673) (Jira IDs: SLS-1429, SLS-1430)
- Resolved an issue that was preventing users from logging in using the default login page if the ***Single Instance Login*** setting was enabled. (Jira ID: SLS-1428)

Business Services

- Resolved an issue where business service status policies were incorrectly calculating the Health state of services. (Case: 00421078) (Jira ID: SLUI-19584)

Credentials

- Updated the SNMP Credential Read/Write fields to display empty fields and values correctly. (Case: 00223980) (Jira ID: EM-49241)
- Resolved an issue that was causing Windows Internet Information Services (IIS) monitoring to fail with the message "Credentials rejected by the server" when monitoring a Windows device using the "Microsoft: IIS Server" PowerPack if concurrent PowerShell collection was enabled and the credentials used included either HOST or WSMAN. (Case: 00393252) (Jira ID: EM-62423)

Data Collection

- Addressed an issue that was causing a "PowerShell Communication" error followed by one or more "PowerShell Request" errors whenever the "pypsrp" Python module was enabled and events relating to a failure to connect to a Windows device were triggered in SL1. With this change, only the communication error is now generated, which is in line with the behavior expected when pypsrp is not being used. (Cases: 00397479, 00419026) (Jira ID: EM-64617)
- Added indexing to the proc_remote_logs database table that significantly reduces on the query time for ModuleCmdStorage, which in turn reduces locks on that table for transactions. (Case: 00427169) (Jira ID: EM-64098)

Events

- Resolved an issue that caused high latency when loading events on the **Events** page. (Case: 00455708) (Jira ID: SLUI-20411)

Global Manager

- Resolved an issue that was causing some Global Manager pages to not load due to child stacks returning an HTTP 502 error, resulting in users having to manually disable monitoring of those child stacks. (Jira ID: SLUI-20184)

Logging

- Updated access logs to ensure the session duration value is correct for expired sessions. (Case: 00323782) (Jira ID: EM-66548)
- When SL1 encounters a device whose neighbor has an IP address that is an empty string, it will no longer create an unhandled exception in the system log. (Case: 00453299) (Jira ID: EM-66229)

PhoneHome Communication

- Addressed an issue that was causing SL1 Collectors in PhoneHome configurations to randomly disconnect from and reconnect to the Databast Server. With this change, SSH authentication for clients having issues will fail quickly, allowing other clients to continue with their own authentication requests. (Case: 00411486) (Jira ID: EM-63308)

User Accounts

- Ensured that the ability to edit the Privilege Keys granted in a user account work as intended. Specifically, if a user has a "user" account type with a defined user policy assigned to their account, then the Privilege Keys section of their **Account Permissions** page (Registry > Accounts > User Accounts > wrench icon > Permissions) should be disabled. (Case: 00421121) (Jira ID: EM-63599)

Recently Deprecated Features

12.2.0

The 12.2.0 release deprecates the following PowerPack and removes it from the ISO:

- Google Base Pack

> **NOTE:** If you are upgrading from a previous version of SL1, the 12.2.3 upgrade will not remove any existing PowerPacks. The PowerPacks listed above are still available for download from the PowerPacks Support page.

12.1.0

- The 12.1.0 release deprecates the following PowerPacks and removes them from the ISO:
    - 3Com Device Classes Base Pack
    - Alcatel-Lucent Base Pack
    - Alteon Monitoring Base Pack
    - APC Base Pack
    - AskEM7 Query Widgets
    - Attachmate Device Classes Base Pack
    - Avaya Base Pack
    - Avocent Base Pack
    - Blue Coat Monitoring Base Pack
    - Brocade: Base Pack
    - Citrix Monitoring Base Pack
    - Citrix: Xen
    - Danaher Device Classes Base Pack
    - DEC Device Classes Base Pack

- Dell EMC: Isilon
- Dell EMC: Unity
- Dell EMC: VMAX and PowerMax Unisphere API
- Dell OM Base Pack
- Dell PowerConnect Base Pack
- Dell PowerVault Event Policies
- D-Link Device Classes Base Pack
- EMC: VMAX
- EMC: VNX
- Empire Device Classes Base Pack
- Enterasys Device Classes Base Pack
- Extreme Base Pack
- Fluke Networks
- Force 10 Monitoring
- Fortinet Base Pack
- Foundry Base Pack
- Google Base Pack
- Hitachi Base Pack
- HP-ISM Base Pack
- HP Pro Curve Base Pack
- HP-UX Base Pack
- Intel Base Pack
- Konica Minolta Base Pack
- LANCOM Systems Device Classes
- Lannair Device Classes
- Lantronix Device Classes
- Liebert Monitoring Base Pack
- Linksys Device Classes
- McAfee Monitoring
- MIB-2 Base Pack

- Microsoft: Azure Classic
- Motorola Device Classes
- NetBotz Base Pack
- NetScout Systems Device Classes
- Netscreen Base Pack
- Nokia Base Pack
- Printer Base Pack
- Riverbed Monitoring
- SMI-S: Array
- SNMP Research Base Pack
- UCD-SNMP Base Pack
- VMware: vSphere Reports
- Vyatta
- Xerox Base Pack

NOTE: If you are upgrading from a previous version of SL1, the 12.2.3 upgrade will not remove any existing PowerPacks. The PowerPacks listed above are still available for download from the PowerPacks Support page.

- With the ***PHP updates*** that were made in SL1 11.1.0, the classic SL1 Global Manager was supported only up to the 10.2.x line. Because the 10.2.x release line has now reached end of life, the ***Classic Global Manager*** manual was deprecated from ***docs.sciencelogic.com***.

11.3.0

- The 11.3.0 release deprecated the following PowerPack and removed it from the ISO:
  - SL1: Concurrent PowerShell Monitor

NOTE: If you are upgrading from a previous version of SL1, the 12.2.3 upgrade will not remove any existing PowerPacks. The PowerPacks listed above are still available for download from the PowerPacks Support page.

Upgrading SL1

IMPORTANT: You can consume SL1 12.2.3 only if you are upgrading from an earlier SL1 version that *supports upgrades to this release*. There is no ISO version for version 12.2.3.

For a detailed overview of SL1, see the *Introduction to SL1* manual.

For detailed instructions on upgrading SL1, see the section on *Updating SL1* in the *System Administration* manual and the upgrade notes that are included in this document.

NOTE: ScienceLogic strongly recommends that you review the *Known Issues* for SL1 (https://support.sciencelogic.com/s/known-issues#sort=relevancy) before installing a new update.

For known issues specific to this release, see the *Known Issues* section of this document.

SL1 Extended Architecture

For existing on-premises deployments of SL1 Extended Architecture, see the section on *Upgrading SL1 Extended Architecture* in the *System Administration* manual for upgrade instructions. For help with technical issues, contact ScienceLogic Customer Support.

Important Upgrade Notes for SL1 Hollywood 12.2.3

This section includes important notes for upgrading existing SL1 systems to the Hollywood 12.2.3 release.

Unless otherwise stated, the information in this section applies to all users who are upgrading from previous SL1 versions.

CAUTION: ScienceLogic strongly recommends that you review these upgrade notes in their entirety before upgrading to version 12.2.3.

Supported Upgrade Paths

Previous SL1 releases included major updates that you must consume before you can upgrade to 12.2.3, if you have not done so already. Therefore, you might be required to upgrade to one or more earlier versions of SL1 before you can upgrade to 12.2.3.

You can upgrade directly to 12.2.3 from the following SL1 versions:

- 12.2.1.1
- 12.2.1.2

If you are currently on SL1 12.1.0 or 12.1.1 and all of your appliances are running on Oracle Linux 8 (OL8), you can upgrade to 12.2.1.2 and then to 12.2.3.

WARNING: For versions 12.2.0 and later, the SL1 platform can be deployed ***only*** on Oracle Linux 8 (OL8) operating systems. This update ensures SL1 can continue to provide key platform security updates and meet rigorous compliance standards while also benefiting users with real-world application performance improvements such as faster database queries and user interface response times.

All customers who are upgrading from a version of SL1 that runs fully or partially on OL7 ***must*** first upgrade to SL1 12.1.2 and then convert all appliances to OL8 before you can upgrade to SL1 12.2.0 or later. If you take no action before October 31, 2024, all older SL1 systems with OL7 will continue to run, but ScienceLogic will not support them, and the systems might not be secure.

For upgrade instructions and important notes about upgrading to 12.1.2, see the *SL1 Golden Gate 12.1.2 Release Notes*.

For more information, see the *OL8 Conversion Resource Center* on the ScienceLogic Support portal, which includes links to numerous resources such as the **Oracle Linux 8 Conversion Guide**. The conversion guide includes prerequisites, instructions for converting to OL8 for all deployment types, FAQs, and other helpful information to walk you through the OL8 conversion process.

Unsupported Upgrade Paths

You cannot upgrade to SL1 12.2.3 in the following scenarios:

- You have not yet deployed or upgraded to an SL1 version in which all appliances are running on Oracle Linux 8 (OL8).
- You are currently on SL1 12.1.2.
- You have an AWS deployment and are currently on SL1 12.1.x using Aurora 3. For more information, see the section on *Aurora 3 Incompatibility*.
- You are on a STIG-compliant deployment of SL1. For more information, see *Known Issues*.

Upgrading MariaDB and Rebooting SL1

Some SL1 versions include important security updates. To apply these updates, you must upgrade MariaDB and then reboot all SL1 appliances.

The following table specifies the required MariaDB version for each SL1 version and which SL1 updates require you to reboot all SL1 appliances:

SL1 Release	Required MariaDB Version	Requires Appliance Reboot?
12.2.3 (Upgrade only)	10.6.18	Yes
12.2.1.2 (Upgrade only)	10.4.31	Yes
12.2.1.1 (ISO only)	10.4.31	N/A
12.2.0	10.4.31	Yes
12.1.2 (OL8)	10.4.31	Yes

SL1 Release	Required MariaDB Version	Requires Appliance Reboot?
12.1.2 (OL7)	10.4.29	Yes
12.1.1 (OL8)	10.4.28	Yes
12.1.1 (OL7)	10.4.29	Yes
12.1.0.2 ISO (OL8)	10.4.28	N/A
12.1.0.2 Upgrade (OL7)	10.4.29	Yes
11.3.2.1	10.4.28	Yes
11.3.2	10.4.28	Yes
11.3.1	10.4.28	Yes
11.3.0	10.4.26	Yes

NOTE: For instructions on updating MariaDB or rebooting the SL1 system, see the section on *Updating SL1* in the *System Administration* manual.

If you would like assistance in planning an upgrade path that meets your security needs while minimizing downtime, please contact your Customer Success Manager.

Aurora 3 Incompatibility

AWS deployments of SL1 on Aurora 3 RDS (MySQL 8.0) are not supported for SL1 12.2.3 or earlier. Aurora 3 support is not currently planned for any future SL1 12.2.x releases.

If you are currently deployed on 12.1.2 or later using Aurora 3, you can upgrade to a 12.3.x release.

Legacy Data Pull Deprecation

SL1 no longer supports the legacy version of Data Pull. If you are upgrading from a version of SL1 prior to 12.2.1.2, you will need to update all of your SL1 appliances to version 12.2.3, including your Data Collectors and Message Collectors, to avoid potential data loss. When all appliances are successfully upgraded to 12.2.3, SL1 will automatically deprecate legacy Data Pull. If you do not update SL1 appliances after 60 days, the data on those appliances will be lost, and you will need to redeploy the appliances.

For version 12.2.3, there is an issue that prevents data pull from properly deprecating older versions; for more information, see the following Knowledge Base article: https://support.sciencelogic.com/s/article/15573. This issue will be addressed in version 12.2.4 and is not present in version 12.3.0.

Future Python 2 Support Deprecation

Prior to SL1 11.3.0, all Dynamic Application snippets, Execution Environments, Run Book Actions, and ScienceLogic Libraries utilized Python 2.

With the introduction of Python 3 support in 11.3.0, ScienceLogic announced its intent to deprecate support for Python 2 in a future release.

Python 2 will become optional in the 12.3.0 release; it will not be installed by default, but can be added during deployment to select nodes or appliances. It will be completely removed from SL1 in the subsequent Q2 2025 release. At that time, customers still using Python 2 will be unable to update to the Q2 2025 release until their custom code is Python 3-compatible.

For more information, see the *Python 3 Resource Center* on the ScienceLogic Support site.

Python 3.9 Execution Environment Support Deprecation

The option to use Python 3.9 execution environments is limited to SL1 12.2.1 and later 12.2.x releases. The SL1 12.3.0 release will remove support for Python 3.9 and add support for Python 3.11.

Any Dynamic Applications that use Python 3.9 execution environments will stop working after upgrading to SL1 12.3.0 or later.

If you are currently using Python 3.9 execution environments, then after updating to 12.3.0 or later, you will need to create a Python 3.11 execution environment and align any Dynamic Applications that are currently aligned to the Python 3.9 execution environments to Python 3.11 execution environment to make them work again.

Enterprise Key Management Service (EKMS) Issues

You might experience the following EKMS-related issues upon upgrading to SL1 12.2.3:

- EKMS might not start due to issues with the configuration files
- EKMS might not start due to an issue where it remains encrypted upon startup.

Both of these issues are described in more detail below.

EKMS Configuration File Issues

In SL1 12.2.1.1 and later, if you are using a high-availability (HA) configuration and you re-ISO or rebuild one of the Database Servers, you might experience an issue where the EKMS vault service (`sl_vault`) does not start due to issues with the configuration files. If this occurs, you will experience the following issues:

- When you attempt to log in to the default user interface (AP2), you will receive an "Unexpected end of JSON" input error.
- When you attempt to log in to the classic user interface, you will receive a "502 Bad Gateway" error.
- The `sl_vault` service gets stuck on the following message: "Error checking seal status: Get "http://localhost/v1/sys/seal-status": dial unix /run/vault/vault.sock: connect: no such file or directory".
- The `/tmp/vault_conf.yml` file displays in plain text and the password displays as `###PASSWORD###`, which indicates that it is not set.

Before attempting to work around this issue, you should first ensure that the `clientdbuser` has the correct permissions. To do so, open an SSH session to the Database Server and run the following command:

```
silo_mysql -e "SELECT user, grant_priv FROM mysql.user WHERE user =
'clientdbuser'"
```

This should return a "`Y`" value. If it does not, contact your database administrator and request permissions for `clientdbuser` before attempting the workaround.

If you have the proper permissions, you can follow these steps to work around this issue:

1. In your SSH session, stop the EKMS services and mask them so they do not restart during the reinitialization:

```
sudo systemctl stop sl_vault sl-vaultmngt
```

```
sudo systemctl mask sl_vault sl-vaultmngt
```

2. Remove the problematic EKMS files:

```
sudo rm -f /tmp/vault_conf.yml /etc/sl_vault/vault_conf.yml /etc/sl_
vault/encryption_key /opt/em7/services/sl_vault/config/hcl/vault.hcl
```

3. Copy the default `vault_conf` template:

```
sudo cp -v /opt/em7/services/sl_vault/utils/vault_conf.yml /etc/sl_
vault/
```

4. Set the permissions for the `vault_conf` file:

```
sudo chown s-em7-security:s-em7-security /etc/sl_vault/vault_conf.yml
```

5. Delete the users. They should regenerate when EKMS reinitializes:

```
silo_mysql -e "DROP USER IF EXISTS 'em7-security'"
```

```
silo_mysql -e "DROP USER IF EXISTS 'em7-security02'"
```

> **NOTE:** You must run this step on both the active and passive Database Servers.

6. Re-enable the EKMS services:

```
sudo systemctl unmask sl_vault sl-vaultmngt
```

```
sudo systemctl start sl_vault sl-vaultmngt
```

EKMS Remains Encrypted Upon Startup

After upgrading to 12.2.1.2 or later, you might experience an issue where the Enterprise Key Management Service (EKMS) for your SL1 system is unable to start because it is still encrypted upon startup.

To check for this issue, use SSH to access your SL1 Database Server and run the following command:

```
sudo cat /tmp/vault_conf.yml
```

If the file is clear text, then this issue does not impact you, and you can ignore the rest of this known issue.

If the file is not clear text, then EKMS is still encrypted and you will need to perform the following workaround steps:

1. Decrypt the vault file:

```
sudo slsctl config --file /etc/sl_vault/vault_conf.yml --key /etc/sl_
vault/encryption_key --decrypt
```

2. Run the command a second time to decrypt the file again, as this issue is caused by a double encryption.
3. Remove the previous configuration file:

```
sudo rm -rf /tmp/vault_conf.yml /opt/em7/services/sl_
vault/config/hcl/vault.hcl
```

4. Restart the `sl_vault` service:

```
sudo systemctl start sl_vault
```

Global Manager Deployment

When deploying or upgrading Global Manager systems, the Global Manager stack and all of its child stacks must run on the same SL1 build version, as well as the same versions of AP2 and Oracle Linux.

Obtaining a ScienceLogic Key for Agent RPM Packages

As of SL1 version 12.1.1, RPM installer packages are now signed. Therefore, when installing an RPM package, you might receive a warning message similar to the following one if the RPM store does not contain ScienceLogic's public GPG key:

```
warning: all silo-agent-x86_64.rpm: Header V4 RSA/SHA512 Signature, key ID
3a6131f6: NOKEY
```

To address or prevent this warning, you can obtain the ScienceLogic key and then add it to the RPM store. To do so:

1. Go to https://keys.openpgp.org/search?q=devops%40sciencelogic.com.
2. Download the key.
3. Import the key into the RPM store using the following command:

```
rpm --import <file name>
```

Validating Agent TLS Connections to the SL1 Streamer Service

As of SL1 12.1.1, customers who use the SL1 Gen 3 agent with on-premises Extended Architecture systems have the option to turn on TLS certificate validation when deploying the Streamer service. This provides additional security to confirm that the agent's connection to SL1 is valid.

To enable this TLS validation, the extended cluster must be configured with a valid TLS certificate and the "requireTls" setting in the Streamer helm chart must be set to "true" when deploying the Streamer, such as in the following command:

```
helm upgrade --version 1.2.13 streamer sl1/sl1-streamer -f output-
files/steamer-values.yml --set requireTls=true
```

If you update this setting, the Streamer pods will restart and the agent will download the new configuration upon its next communication with the cluster.

CAUTION: This TLS validation is currently disabled by default for on-premises Extended Architecture deployments.

If you want to enable this feature, it is important to first ensure that the Streamer end point that is provided via the URLFRONT installation option is configured with a valid TLS certificate. If the agent is configured to validate the TLS connection but the cluster it is trying to communicate with does not have a valid TLS certificate, the agent will be unable to communicate with that cluster.

If this occurs, you can disable the validation by updating the Streamer deployment to disable the "requireTls" setting, updating the scilog.conf file to remove or alter the "RequireWebCert true" line, and then restarting the agent.

NOTE: This feature can be enabled on SaaS SL1 deployments by submitting a Service Request case to the SRE queue at the ScienceLogic Support site at https://support.sciencelogic.com/s/, or by contacting your ScienceLogic customer service manager.

System Update Notes

- ***SL1 updates overwrite changes to the configuration file /opt/em7/nextui/nextui.env***. This is a known issue. (For more details, see https://support.sciencelogic.com/s/article/1161 and https://support.sciencelogic.com/s/article/1423.) ScienceLogic recommends that you back up this file before applying an update and then reapply your changes to this file.
- The SL1 user interface will be unavailable intermittently during system update.
- 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 SL1 releases during a maintenance window.
- The SL1 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.

Verifying PowerPack Version Compatibility

Before consuming SL1 12.2.3, please verify whether any PowerPacks currently running on your system are newer than the PowerPacks included in this release.

If the PowerPack on your system is newer than the one included with this release, you might see spurious error messages.

To avoid spurious error messages:

1. Before installing the SL1 update, go to the **Device Components** page (Registry > Devices > Device Components).
2. Find each root device associated with the PowerPacks you do not want to update and select their checkboxes.
3. Click the ***Select Action*** field and choose *Change Collection State: Disabled (recursive)*, and then click the **[Go]** button.
4. Wait five minutes after disabling collection.
5. Install the SL1 update.
6. After the SL1 update is complete, go to the **Device Components** page (Registry > Devices > Device Components).
7. Select the checkbox for all affected root devices.
8. Click the ***Select Action*** field and choose *Change Collection State: Enabled (recursive)*, and then click the **[Go]** button.

Upgrading from Oracle Linux 7 (OL7) Versions of SL1

If you are upgrading from a version of SL1 prior to 12.2.0 and first need to upgrade to 12.1.2 and/or convert all of your SL1 appliances to Oracle Linux 8 (OL8), ScienceLogic ***strongly*** recommends that you review the *Important Upgrade Notes* section of the *SL1 Golden Gate 12.1.2 Release Notes* prior to upgrading.

Known Issues for SL1 Hollywood 12.2.3

NOTE: ScienceLogic strongly recommends that you review all Known Issues for SL1. For more information, see https://support.sciencelogic.com/s/known-issues#sort=relevancy.

The following known issues exist for SL1 Hollywood 12.2.3:

- Users on STIG-compliant deployments of SL1 cannot upgrade to 12.2.3. This is due to a MariaDB database vendor defect that impacts only STIG-compliant deployments that can spawn duplicate component devices at a rate that can impact SL1 performance or overload the system. ScienceLogic is working to address this issue.
- AWS deployments of SL1 on Aurora 3 RDS (MySQL 8.0) are not supported for SL1 12.2.3.
- When upgrading SL1 on AWS stacks, you might receive an error message that the Data Engines failed to patch correctly. If this occurs, re-run the pre-upgrade tests and then run the patch again; this should result in the Data Engines updating correctly and the correct version then being reflected on the **Appliance Manager** page (System > Settings > Appliances).

- After upgrading, to ensure proper data collection, you should go to the **Appliance Manager** page (System > Settings > Appliances), locate one of the Data Collector or Message Collector appliances, and click the lightning bolt icon to force configuration push for that appliance.
- The preupgrade expiry check might fail for Database Servers that utilize out-of-the-box licenses, even when the license is set to expire after the configured expiration period. This issue does not impact appliances that use licenses procured from ScienceLogic. For more information, including a workaround for this issue, see: https://support.sciencelogic.com/s/article/12914. (Jira ID: EM-61746)
- When upgrading a large number of SL1 appliances, you might encounter an issue where the deployment summary shows that deployment timed out for many of the appliances but, upon further inspection, you discover that the appliances actually deployed correctly. This is due to a lag in the deployment status reaching the Database Server after the default timeout value of 3600 seconds (1 hour). If you check back later, the issue should fix itself. If you would rather work around this issue, you can increase the timeout value. For instructions, see the section on ***Adjusting the Timeout for Slow Connections*** in the "***Updating SL1***" chapter of the ***System Administration*** manual. (Jira ID: EM-62316)
- After updating your Database Server and/or Administration Portal passwords using the Web Configuration Utility on port 7700, you might experience an "Unexpected end of JSON input" error when you attempt to log in to the default SL1 user interface (AP2). To work around this issue, use SSH to access the Administration Portal and run the following commands as "sudo", replacing `<password>` with the appropriate password:

  ```
  sl1-config -y -q silo CENTRAL dbuser clientdbuser

  sl1-config -y -q silo CENTRAL dbpasswd <password>

  sl1-config -y -q silo CENTRAL ap_user apuser

  sl1-config -y -q silo CENTRAL ap_pass <password>
  ```

  (Jira ID: EM-64285)
- In SL1 12.2.1.1 and later, if you are using a high-availability (HA) configuration and you re-ISO or rebuild one of the Database Servers, you might experience an issue where the EKMS vault service (`sl_vault`) does not start due to issues with the configuration files. If this occurs, when you attempt to log in to the default user interface (AP2), you will receive an "Unexpected end of JSON" input error; if you attempt to log in to the classic user interface, you will receive a "502 Bad Gateway" error. For more information including a workaround, see the upgrade note about ***EKMS issues***. (Jira ID: EM-66594)
- After upgrading to 12.2.1.2 or later, you might experience an issue where the Enterprise Key Management Service (EKMS) for your SL1 system is unable to start because it is still encrypted upon startup. For more information including a workaround, see the upgrade note about ***EKMS issues***. (Jira IDs: EM-66508, EM-66487)

- Some upgraded 12.2.x instances do not have `api_expanded` option listed for the `eventmanager` in the `silo.conf` file, which in turn is causing Zebrium events to not trigger in SL1. To work around this issue:

  1. Either go to the console of the SL1 appliance or use SSH to access the SL1 appliance.
  2. Open a shell session on the server.
  3. Type the following at the command line:

     ```
     sudo visilo
     ```

  4. Locate the line for "eventmanager" and update it to include "api_expanded". For example:

     ```
     eventmanager = internal,api,dynamic,syslog,trap,api_expanded
     ```

  5. To save your changes and exit the file, enter `:wq` and then confirm that you want to save.

  (Jira ID: SLUI-18754)

- On SL1 Oracle Linux 8 (OL8) appliances, after upgrading or after deploying a new HA, DR, or HA+DR stack, the following WARNING messages might appear when issuing commands using crm or any script/utility that utilizes crm, such as:

  ```
  WARNING: could not get the pacemaker version, bad installation?
  ```

  ```
  WARNING: list index out of range
  ```

  These warnings can be safely ignored. For more information, see: https://support.sciencelogic.com/s/article/14388. (Jira ID: EM-63091)

- If your SL1 system is running Windows 2008 or Windows 2012, and you are using PowerShell collections that have the ***Encrypted*** field set to *Yes* in the credentials, those collections will stop working. For more information, see *Users with Windows 2008 R2 Servers or Windows 2012 Servers* in the SL1 Product Documentation. (Jira ID: EM-61204)

- After installing or upgrading to SL1 12.2.3, each time the system status script (system_status.sh) runs, you might notice that error/traceback messages appear stemming from the SL1 siloupdate service. These messages can be safely ignored. For more information, see: https://support.sciencelogic.com/s/article/11591. (Jira IDs: EM-59277, EM-65832)

- In AWS Extended Architecture upgrade deployments, the active Data Engine might display a banner message that indicates there is no active database after a failover has been performed. If there appear to be no other issues and everything otherwise seems to be working as expected, check the database for the following file: /data.local/tmp/motd.pid. If that file exists, delete it and wait for motd to run again. After it runs again, you can log out and log back in. The banner message should no longer appear. (Jira ID: EM-59194)

- A known issue might cause high swap usage in excess of 95% to be observed on appliance types running SL1 12.1.x and Oracle Linux 8. This impacts all appliance types, but is most frequently observed on Database Servers or appliances that are under heavy memory pressure. For more information about this issue, including a workaround, see: https://support.sciencelogic.com/s/article/11598. (Jira ID: EM-59269)

- A known issue might cause several log configuration files to conflict, which could cause you to see errors for the `sl_vault` and `slsctl` logs or potentially block log rotation in some cases, depending on the order in which the files are executed. To work around this issue, delete the config files `~sl_vault` and `~slsctl`. (Jira IDs: SLS-1105, EM-62134)
- When using the SNMP Public V2 credential to discover devices, you might see an unhandled exception in the system log near the end of the discovery session, despite the devices being discovered successfully. (Jira ID: EM-59380)
- A known issue is causing PDF and XSLX Ticketing report types to fail to generate properly due to an OL8 incompatibility issue. For more information, see: https://support.sciencelogic.com/s/article/11649. (Jira IDs: EM-51131)
- After upgrading to 12.2.x, you might be unable to delete devices from the **Devices** page. If this occurs, you can work around this issue by deleting the device from the **Device Manager** page in either the current ("AP2") SL1 user interface (Devices > Device Manager) or the classic user interface (Registry > Devices > Device Manager), or you can delete the device from the Database Server. (Jira ID: EM-62874, Case: 00412497)
- The following known issues impact Business Services:
    - The **[Anomalies]** tab on the **Service Investigator** page for device services might incorrectly display devices that have anomaly detection disabled, rather than showing only those devices with anomaly detection enabled. (Jira ID: EM-62884)
    - Organizations must have at least one or more accounts assigned to them to ensure the relevant services are saved. (Jira ID: SLUI-17810)
    - For services that have their ***RCA Options*** field enabled, and has had a child service removed, SL1 will not compute the health, availability, and risk values until the Service Topology Engine returns an updated topology, which occurs every 5 minutes by default. (Jira ID: SLUI-18853)

      IMPORTANT: Before deleting child services in a 3-tier hierarchy, check if the parent service has the ***RCA Options*** field *Enabled*, then set this field to *Disabled* if it is not already.

- In new installations of SL1 12.2.3, the "EM7 Web Server" PowerPack that is normally installed by default is not being installed. You can manually install this PowerPack after SL1 has been installed and configured. For instructions, see the section on ***Installing a PowerPack*** in the ***PowerPacks*** manual. This issue does not impact SL1 instances that have been upgraded from earlier releases. (Jira ID: SOL-24609)
- The "Oracle: Database" PowerPack v105 will not work on SL1 12.2.3 because of a known issue regarding the Oracle client cx_oracle. This be will addressed in a future release. (Jira ID: EM-64241)
- "VMware: vSphere Base Pack" PowerPack v306 and v307 are not compatible with SL1 12.2.3 or other SL1 deployments that are running on Oracle Linux 8 (OL8). This incompatibility was addressed in v308 of the PowerPack. (Jira ID: SOL-24062)

- The CyberArk credential gateway service integration is incompatible with SL1's Concurrent PowerShell feature. If you are using the CyberArk credential integration, you must have Concurrent PowerShell disabled. To disable Concurrent PowerShell, go to the **Behavior Settings** page (System > Settings > Behavior), ensure that the ***Enable Concurrent PowerShell Collection*** checkbox is not selected, and click **[Save]**. (Jira ID: EM-63205)
- The **[Expand]** and **[Contract]** buttons are not working as intended on the **Dynamic Application Collections** page (Devices > Device Manager > wrench icon > Collections). You can still expand and contract individual items on the page. (Jira ID: EM-64420)

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com. For more information, see https://sciencelogic.com/company/legal.

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010