ScienceLogic

SL1 Hollywood 12.2.1.1 Release Notes

SL1 version 12.2.1.1

SL1 Hollywood 12.2.1.1 Release Notes

IMPORTANT: SL1 12.2.1.1 replaces the previous 12.2.1 release.

If you are upgrading from a release of SL1 prior to 12.2.1.x, you cannot upgrade to 12.2.1.1; you must download and upgrade to the upcoming version 12.2.1.2. You can only consume SL1 12.2.1.1 if you are performing a fresh installation of SL1.

The SL1 Hollywood 12.2.1.1 release includes the following new features and enhancements:

- A new *"Custom" widget dashboard widget type* that enables you to add HTML content to your widgets
- New *custom Device Investigator layouts and alignment types*
- A *Masked Events modal* that you can access from the **Events** page
- A new *Density setting* for inventory pages in the default user interface
- Plus *many additional updates*

IMPORTANT: As of version 12.2.0, SL1 no longer supports deployment on Oracle Linux 7 (OL7).

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

To view the features, enhancements, and addressed issues that are included in previous SL1 Hollywood releases, see the following release notes:

- *12.2.0*

This document covers the following topics:

New Features and Enhancements in SL1 Hollywood 12.2.1.1

Dashboards

- **What's new:** ***A new Custom dashboard widget type for HTML content.*** Added a new **Custom** widget type that you can select on the **Create Widget** page that provides a user interface-only visualization. For this release, the **Custom** widget has a single *HTML Widget* visualization option, which can render any rich content or HTML that you input. The following additional changes were made to support this new feature:
    - You can view or edit HTML content directly in the text editor. You can do this either in the **[Basic]** tab, which allows you to update the widget by editing plain text directly, or in the **[Advanced]** tab, which allows you to view and edit the raw HTML content.
    - To open the code view, you can either click the **[Advanced]** tab or click the ellipses button (⋮) on the top-right corner of the **Preview** pane and then select *Code View* (<>).
    - You can link a dashboard to the HTML widget by enabling the ***Title links to another page*** toggle, selecting *Dashboards* from the ***Link Type*** drop-down field, clicking the ***Choose Dashboards*** hyperlink, and then selecting one or more dashboards in the **Choose a Dashboard** modal that appears.
    - You can link a URL to the HTML widget by enabling the ***Title links to another page*** toggle, selecting *Advanced URL* from the ***Link Type*** drop-down field, then copying and pasting the URL you want to link into the ***Link URL*** field.
    - Color themes were updated for **Custom** widgets that are using the *HTML Widget* visualization.
- **For more information:** See *Creating Dashboard Widgets*.

Additional Dashboards Updates

- Added a new *Last 2 days* option to the **Time span filter** drop-down field on the **Dashboards** page.
- You can now integrate third-party tools into SL1 with external linking. To do so, toggle on **Items link to another page** when creating widgets. When you do so, two additional fields will appear, ***Link base URL*** and ***Link Tooltip***. This new feature supports the following widgets and their corresponding visualization options:
    - **Device** widgets that have *Leaderboard* or *Table* visualizations.
    - **Interface** widgets that have *Leaderboard* or *Table* visualizations.

Devices

- **What's new**: ***Custom Device Investigator layouts and alignments***. Added the ability to view details about custom **Device Investigator** layouts, as well as the ability to bulk align layouts that you own to specific device categories, device classes, and devices.

  > **NOTE:** Layouts and layout alignments can be private, which are owned by a specific user, or public, which are available to everyone. The alignment type defaults to either private or public based on the selection made in the most recently edited alignment.

  The following updates were made to support this enhancement:

  - Added a **[Choose Layout]** tab when you click the **[Edit]** (layout) button from the **Device Investigator**. This tab includes a list of existing **Device Investigator** layouts that you own or have access to. You can change the **Device Investigator** layout that is currently aligned to that device by clicking the radio button for a different layout.
  - Added a new **Device Investigator Layouts** page (Devices > Device Investigator Layouts), where you can view a list of the existing **Device Investigator** layouts that you own or have access to. You can also access this page from within the **Device Investigator** by clicking **[Edit]** (layout) > Choose Layout > Manage Layouts. This page includes the following information about each layout:
    - Layout name, ID, and owner
    - The number of device categories, device classes, and devices aligned to each layout
    - The date and time the layout was last edited, as well as the user responsible

    > **NOTE:** To view this page, your user account must be aligned to an access key that includes the DEV_VIEW access hook. To delete **Device Investigator** layouts from this page, your user account must have an access key that includes the "DEVICE_INVESTIGATOR_REMOVE" or "DEVICE_DASH_EDIT" access hooks.

  - From the **Device Investigator Layouts** page, you can click the ***Layout Name*** link for a particular layout to view or filter the list of specific device categories, device classes, and devices that are aligned to that layout. If you are the layout owner, you can also edit the layout name or its alignments.
- **For more information**: See *Using the Device Investigator*.

Additional Devices Updates

- Added a new **Relationships** widget to the **Device Investigator** that displays details about the other devices and services that have relationships to the selected device.

  NOTE: The **Relationships** widget is hidden by default in SL1 12.2.1.1. You can enable the widget using the following GraphQL mutation:

  ```
  updateFeatureToggle(id: "system:AP2_DEVICEDETAIL_RELATIONSHIP_
  TAB", value:"enabled")
  ```

  If you previously installed the AP2 Croissant version 8.5.7 release, then when you install SL1 12.2.1.1, which includes the AP2 Doughnut version 8.6.30 release, the **Relationships** widget will disappear from any existing **Device Investigator** layouts. To re-enable it, use the above GQL mutation.

- Made the following updates to the **[Collections]** tab of the **Device Investigator**:
  - Added a new ***ID*** column that displays the globally unique ID number (GUID) of each Dynamic Application listed on the page.
  - Added a new ***Numeric ID*** column that displays the numeric integer ID number of each Dynamic Application listed on the page. This numeric ID can be used to correlate Dynamic Applications to their error logs.
- Made the following updates to the **[Events]** tab of the **Device Investigator**:
  - The ***ID*** column is now labeled ***Event ID***.
  - Columns were added for ***Masked Events*** and ***Automated Actions***.
- The "EM7 Core: Async Device Deletion" process, which was deprecated in earlier releases, has been removed from SL1.

Events

- **What's new: *The Masked Events modal*.** Added a new **Masked Events** modal that you can access from the **Events** page. On the **Events** page, any event that contains masked events includes an icon ( ) that you can click under the ***Masked Events*** column. You can click this icon to open the new **Masked Events** modal.

  The following updates were made to support this enhancement:

  - The **Masked Events** modal displays the same events table from the **Masked Events** widget on the **Event Investigator** page. This modal also contains an event overview, which you can still access from the **Event Overview** widget on the **Event Investigator** page. You can perform all the same functions in this modal as you would be able to in the **Masked Events** widget, and the **Event Overview** widget on the **Event Investigator** page.

    - You can access the **Masked Events** modal in SL1 Global Manager systems for Business Services.
- **For more information**: See *Viewing Events*.

Additional Events Updates

- You can now add color-coded highlights to rows on the events inventory table that correspond to the severity color of the event. To do so, go to the **Events** page, click the **[View]** drop-down field, then switch the toggle on for *Highlight rows by severity* option.
- You can now perform a bulk action for editing event notes on the **Events** page.
- Removed the webhook container service from SL1 and replaced it with a new RPM that gets installed as part of the SL1 upgrade. The webhook collector service no longer appears in Docker images or containers on SL1 Message Collectors or All-in-One Appliances. Also added a `systemd` alias so that `systemctl` commands work for both service names (`webhook-collector` and `webhook_collector`) for backwards compatibility. For example, the commands `sudo systemctl webhook-collector` and `sudo systemctl webhook_collector` provide the same output.

User Interface

- **What's new: *A Density setting for inventory pages***. Added a new *Density* setting to the gear icon and ellipses drop-down field that appear at the top of all inventory pages. This setting enables you to switch between two settings:
    - ***Compact***, which uses less padding between rows and a smaller font size.
    - ***Comfortable***, which uses more padding between rows and a larger font size.
- **For more information**: See *Adjusting Row Density*.

Additional User Interface Updates

- The following inventory pages and tabs in the SL1 user interface have been updated to use a new set of filters for the columns in the list. You can start typing filter text or select filter options in one or more of these filters to narrow down the list to just the items you want to view:
    - **Service Templates page** (Business Services > Templates)
    - **Policy Editor page** (Enhanced Service Investigator > Status Policy)
    - **Maps page** (The **[Maps]** tab on the left-side navigation menu)
    - **Maps window** (Maps > Create Maps)
    - **Add Node window** (Maps > Add Node)

Additional New Features and Enhancements in SL1 Hollywood 12.2.1.1

Access Hooks and Keys

- Added the access hooks DEV_NOTES_ADD, DEV_NOTES_EDIT, and DEV_NOTES_REMOVE. These hooks enable users to add, edit, and delete device notes, respectively.

Agent

- Improved agent performance by adding a "heartbeat" request that regularly updates the Streamer service with agent summary data.

API

- Deprecated the PHP REST API headers with the prefix "x-em7" and replaced them with the preferred "x-sl" prefixed headers. Support for "x-em7" headers will be removed in a future release.

Authentication

- The tmux utility now runs by default when you access an SL1 system using SSH. The addition of this utility, which is a terminal multiplexer that enables a number of terminals to be created, accessed, and controlled from a single screen, strengthens session-control mechanisms and aligns with industry-wide security practices. With this update, sessions are automatically locked after 15 minutes of idleness or if an unclean SSH disconnect or dropped SSH connection occurs. Upon login, SL1 checks for and attaches any detached tmux session if it finds them; otherwise, it starts a new session. This update also introduces advanced features like scroll-back buffering with search, built-in clipboarding, multiple sessions and panes, detaching or attaching sessions, and session supervision or sharing. For more information about tmux shortcuts and usage, see https://tmuxcheatsheet.com/.

Business Services

- The enhanced **Service Investigator** page is now enabled by default. ***This page was originally introduced in SL1 12.2.0*** but was disabled by default in that release.
- When creating status policies for business services, *Percent* will now appear under the ***Aggregate*** drop-down field. If you select this option and one or more devices in your service are unavailable, SL1 will display the number of unavailable devices as a percentage of the total number of devices for that particular service.
- Any time range you select in the ***Timeline*** panel will no longer count duplicate events. For instance, if you have the same event occur at two separate times, and the time range you select includes the two times that event occurred, the panel will count only one of the events.

> **NOTE:** You can go back only 24 hours when clicking the back icon on the ***Timeline*** panel.

Data Collection and Retention

- When the "Data Collection: SNMP Collector" and "Data Collection: PowerShell Collector" processes are disabled on the **Process Manager** page (System > Settings > Admin Processes), the following options are also disabled in the user interface to ensure that concurrent SNMP and concurrent PowerShell cannot be used:
    - The ***Enable Concurrent SNMP Collection*** and ***Enable Concurrent PowerShell Collection*** fields on the **Behavior Settings** page (System > Settings > Behavior)
    - The ***Enable Concurrent SNMP Collection*** and ***Enable Concurrent PowerShell Collection*** fields on the **Edit Collector Group** modal (Manage > Collector Groups > Actions > Edit Collector Group)
- Added primary keys to specific database tables to improve performance of queries during medium-frequency collection. The improved queries prevent medium-frequency collection from falling behind and causing an outage.

Global Manager

- Enabled Security Assertion Markup Language (SAML) as an option for single-sign-on (SSO) authentication for Global Manager using GraphQL.

GraphQL

- Added GraphQL support for a "run-as" header, `x-sl-run-as`, that enables administrators to run queries and mutations as a different, non-privileged user. This header is available for use to administrators only; any other users who attempt to use it will receive a 401 error.
- Made the following GraphQL updates to support the enhancements to **Device Investigator** layouts:
    - Added an `alignedDeviceInvestigatorLayouts` field to the `device`, `deviceClass`, and `deviceCategory` objects.
    - Enhanced `DeviceSearch`, `DeviceClassSearch`, and `DeviceCategorySearch` with a new `alignedDeviceInvestigatorLayout` field.
    - Added a new `deviceInvestigatorLayoutAlignment` node that includes fields such as `id`, `parentType`, `parentId`, `user`, `layoutId`, `editedBy`, and `editedDate`.
- To support the new **Relationships** widget for the **Device Investigator**, added a new `DeviceInvestigatorLayoutRelationshipInput` field that can be included in layout arguments for the `createDeviceInvestigatorLayout` and `updateDeviceInvestigatorLayout` mutations.
- Added a new `convertDynamicAppGuidToNumericId` query that returns the numeric integer ID for a Dynamic Application from its GUID.
- Added a new `statistics` category to the `aiMachineLearningMetricAnomalies` node to improve the performance of AI/ML prediction metric GQL queries. This category includes two new fields, `anomalyCount` and `maxAnomalyScore`, which are calculated over a provided `timeSpan` input.
- Added a `LinkedMetric` GraphQL node for events.

Logging

- Ensured that all actions that renew the SL1 session ID are logged in the audit log.
- General audit log entries are now created whenever POST requests are submitted to the SL1 classic user interface. Auto-refreshing pages that use POST requests to refresh themselves will not create audit log entries.
- Improved logging around timeouts for the "Enterprise Database: Collector Config Push" process (config_push.py).

Platform and Security

- SL1 version 12.2.1.1 includes multiple package updates to improve security and system performance. Included among these package updates is an upgrade to Kafka 3.6.0.
- Additional core SL1 features have now been updated to support Python 3. Unless otherwise noted in the SL1 documentation, this does not result in any behavior changes.
- Added a new **Security** page (System > Settings > Security) in the classic SL1 user interface. This page includes:
    - A new Verify TLS Certificates checkbox. When selected, SL1 services will validate TLS certificates that are presented to them. Any self-signed certificates will be rejected when this setting is enabled.
    - An Enterprise Key Management System (EKMS) section that includes the status and current status message for the EKMS service.
- Updated the login banner to display the last successful login date and time stamp to ensure a user's account has not been compromised.
- Updated mysql_establish_grants.py code to allow passwords to contain special characters and eliminate characters that cause login issues.
- Removed the "Application Management: Service Management Engine" system process from SL1. This process was related to a long-deprecated SL1 feature.

PowerPacks

- The following updated PowerPacks are included in SL1 12.2.1.1:
    - Data Pull Support v8.6.0
    - Linux Base Pack v110
    - ScienceLogic Support Pack v107
    - SL1: Performance Reports v103

- Version 8.6.0 of the "Data Pull Support" PowerPack includes the following new metrics in the "Storage Tasks" Dynamic Application types:
    - Compression Errors
    - Deprecated Storage Format Errors
    - Store Errors
    - Unknown Message Format Errors
    - Unknown Message Version Errors
    - Unpack Errors
    - Unsupported Header Errors
- The "ScienceLogic Support Pack" v107 PowerPack includes the following updates:
    - Added a new "Support: Dynamic App Sigterm Report," which can be accessed by going to Reports > Run Report > Support > Support: Dynamic App Sigterm Report.
    - Dynamic Applications are now aligned to either a root device or an assigned Data Collector and not just to "default".
    - Updated the "Support: Appliances Validation" Dynamic Application so that it will only alert on the Database Server and not on the data engines for SaaS SL1 deployments.
    - Removed the "Support: DB Space Estimator" Dynamic Application from the PowerPack. Database space predictions and related log messages are no longer generated.
    - Update the SQL queries for reserved keywords in the PowerPack to be MariaDB 10.6-compliant.
    - The "Support: MariaDB Configuration" Dynamic Application now checks for a correctly sized max_allowed_packet MariaDB variable.
    - The "Support: Slow Query Check" Dynamic Application is now deprecated and disabled by default.

ScienceLogic Libraries and Execution Environments

- Built-in, non-snippet Dynamic Application types now use a pre-deployed, read-only Python 3 execution environment, "sl1_default_ee". This execution environment appears on the **Environment Manager** page (System > Customize > ScienceLogic Libraries > Actions button > Execution Environments), but you cannot edit or delete it. Whenever new, built-in Dynamic Applications are created via the user interface, they will be automatically assigned to this execution environment.

> **NOTE:** As part of this update, the internal collection processes and Internal Collection Dynamic Applications (ICDAs) now run on Python 3. The snippet code that is included in these Dynamic Applications must be Python 3, or at least Python 2/3-compliant.

- You can now align Dynamic Applications to Python 3.9 execution environments.

> **NOTE:** The option to use Python 3.9 execution environments is limited to SL1 12.2.1.1 ***only***. This option will not be available in future versions of SL1, which will add support for Python 3.11 execution environments. Any Dynamic Applications that use Python 3.9 execution environments will stop working after upgrading to SL1 12.2.2 or later. In that scenario, you would need to create a Python 3.11 execution environment and align the Dynamic Applications to that execution environment to make them work again.

System Updates

- The SL1 product update (siloupdate) process added a new "[DATAPULL] allow_legacy_storage_objects = 1" option when importing a patch that changes the data pull message format. This option reverts to its previous state when the entire stack is compatible with the new message format.

Topology

- You can now collect Layer 2 and Layer 3 topology relationships via Address Resolution Protocol (ARP) table data. This functionality is disabled by default. To enable this functionality, you must use the parameter "use_arp" with a value of "1" in the master.system_settings_core database table.
- You can now use device names to create CDP and LLDP relationships. This functionality is disabled by default. To enable this functionality, you must use the parameters "cdp_device_name_search" and "lldp_device_name_search", respectively, with values of "1" in the master.system_settings_core database table.
- Made updates to prevent unhandled exceptions from occurring when non-string ("None") GUID and Unique_ID values are collected in DCM+R relationships.

Issues Addressed in SL1 Hollywood 12.2.1.1

This section describes the issues that were addressed in SL1 Hollywood 12.2.1.1.

Agent

- For Linux agents, the directory /var/log/jmx-collector is now created with 774 permissions, and the log file in that directory is created with 666 permissions. The /var/log/scilogd.log file will also have 774 permissions. When the agent is uninstalled, users should ensure that the /var/log/jmx-collector and /tmp/scilog directories and the /var/log/scilogd.log file are all removed. (Case: 00414437) (Jira ID: EM-63094)
- Addressed an issue with the Windows agent where monitoring the Windows Event logs would sometimes result in duplicate log messages in SL1. (Case: 00419211) (Jira ID: AP-2579)
- Ensured that, when disks or file systems are added or removed, the agent will upload a new system inventory file, which updates that data in SL1. (Case: 00416753) (Jira IDs: AP-2760, AP-2761)

- Resolved an issue that was causing the agent to not correctly report the addition of new network devices. Additionally, Windows interfaces will now show the adapter name instead of the old adapter GUID. (Case: 00399443) (Jira IDs: AP-2722, AP-2723)
- The Linux agent now supports running the agent as non-root in Solaris environments to report the list of running processes, rather than only reporting the agent process itself. (Case: 00374670) (Jira ID: AP-2715)

Authentication

- Made updates to ensure that, if you are on a specific page in SL1 and have to log back in using the single sign-on login page, SL1 returns you to the page you had previously been on rather than your default landing page. (Cases: 00291753, 00415130) (Jira IDs: SLUI-11054, SLS-1065)
- Resolved an issue that was causing some users to receive an "Internal Server Error" after upgrading. (Jira IDs: EM-62105, EM-62529, EM-63490)
- Addressed an issue that was sometimes causing a spinning "loading" circle or an error that prevented users from logging in again if they repeatedly signed in and out of SL1 in a short period of time. (Jira IDs: SLUI-15357, SLS-1169)

Business Services

- Addressed an issue that prevented newly created Bandwidth Billing policies from showing any collected data in the performance graph or interface billing report after upgrading to 12.1 or later. (Case: 00411921) (Jira ID: EM-62873)
- Resolved an issue where the "Health," "Availability," and "Risk" field values were displaying "Unknown" due to gaps in data sets across business services and timeouts in GraphQL requests. (Case: 00382593) (Jira ID: SLUI-18636)
- Addressed an issue that was causing the ***RCA Options*** field to be disabled by default in services that were added to or created in N-tier hierarchies. (Jira ID: SLUI-18852)

Credential Management

- The SL1 credential gateway service now allows you to custom define a CyberArk delimiter when sourcing credential data from external CyberArk vaults. Previously, if you used a password that included a comma, that password would be truncated and therefore incorrect. With this change, you can now set a custom delimiter as something other than a comma so you can use commas in CyberArk vault passwords. For more information, see the section on *Using External Credential Services*. (Case: 00392089) (Jira ID: EM-62338)
- When sourcing credential data from an external CyberArk vault, the credential gateway service no longer requires repository access to install and run. (Case: 00412933) (Jira ID: EM-62959)

Dashboards

- Event and Device Group table widgets now limit queries to a maximum of 1,000 devices at a time to prevent scenarios where no data displays due to the system trying to query too many devices at once. (Case: 00324585) (Jira ID: EM-62026)

- Updated the Quick Time Selector in classic dashboards to ensure the system uses the time zone value based on the user's account settings. (Case: 00374769) (Jira ID: EM-61099)
- Addressed an issue where the "Device Table" widget on the "Dashboards" page for the "Cisco: Meraki [API]" PowerPack was not displaying data. (Case: 00396156) (Jira ID: SLUI-18788)

Data Collection and Retention

- Addressed an issue where orphaned data would remain behind in the database and cause issues with duplicate data being displayed in the user interface. (Case: 00331438) (Jira ID: EM-61266)
- Resolved an issue with the "ScienceLogic Support Pack" PowerPack that was causing the "Support: Async Message Backlog Performance" Dynamic Application to report values under the incorrect label. (Cases: 00293993, 00369218) (Jira ID: EM-54030)
- Added an optimization for a query that gets expired collection objects as part of hourly maintenance, resulting in faster query speed. (Case: 00390557) (Jira ID: EM-61999)
- Addressed an issue that caused the "EM7 Core: Frequent Maintenance" process to trigger unhandled exception errors when handling report statuses. (Cases: 00306662, 00368824, 00386046) (Jira ID: EM-55146)
- Resolved an issue that prevented Daily Maintenance from pruning data for deleted or purged devices. (Case: 00350321, 00330933) (Jira ID: EM-58685)
- Updated the Configuration Data Pruner to delete rows that are older than the data retention setting and that have "None" as the last known configuration data point. (Case: 00263126) (Jira ID: EM-52516)
- Resolved an issue that was causing "Deadlock found when trying to get lock" unhandled storage object exceptions to appear in the system log during nightly auto-discovery. (Case: 00312079) (Jira IDs: EM-56187, EM-56396)

Deployment

- Addressed an issue in which passwords that contained special characters caused boot failures during installation. (Case: 00405322) (Jira ID: EM-62493)

Device Management

- Audit logs will now display when you update interface collection states. (Case: 00271905) (Jira ID: EM-53286)
- Improved the efficiency with which devices can be deleted on systems that have a large number of dynamic rules. (Case: 00377609) (Jira ID: EM-61320)
- Improved the performance of the **Device Investigator** when many events are present. (Case: 00413105) (Jira ID: SLUI-19177)

Discovery

- Addressed an issue that caused an unhandled exception error to trigger during device discovery when invalid IP addresses were collected from a device. (Cases: 00293495, 00337093, 00415532) (Jira ID: EM-54502)

- An alert message in the Device Logs no longer triggers for port scanning during discovery if port scanning is disabled for discovery. (Case: 00310312) (Jira ID: EM-55508)
- Duplicate discovery sessions no longer appear in the **Discovery Control Panel** page of the classic user interface. (Case: 00362309) (Jira ID: EM-59610)
- If the ***Dynamic Discovery*** checkbox is left unselected on a Device Template, it will no longer align during manual rediscovery or nightly auto-discovery. (Case: 00248130, 00241533) (Jira ID: EM-50462)
- Resolved an issue that was preventing network interface discovery from completing correctly due to an error indicating that "MySQL has gone away." (Case: 00406155) (Jira ID: EM-62521)
- You can no longer delete a device class if it is aligned to a device. (Case: 00310455) (Jira ID: EM-55203)
- You can now increase the timeout for SSL discovery higher than the default 1 second value. (Case: 00281513) (Jira ID: EM-54153)

Events

- Addressed an issue that was causing the **Event Insights** page to not loading properly in AWS Extended Architecture deployments and to display incorrect "No Event Created" metrics for multiple deployment types. (Jira IDs: EM-58561, EM-59467)
- Resolved several issues that were preventing event suppressions from working on devices in device groups. (Cases: 00365084, 00376097, 00377769, 00379446) (Jira IDs: EM-60418, EM-60621, EM-61157)
- Updated the database connection to prevent the webhook collector service from becoming unresponsive. (Case: 00347608) (Jira ID: EM-58683)
- When a trap alert spike occurs, alert removal no longer causes the "remove_spike_messages_trap" unhandled exception to occur on the "EM7 Core: Event Processing Engine" system process. (Cases: 00379231, 00379836) (Jira ID: EM-61152)
- Updated the "Support: Async Message Backlog Performance" Dynamic Application so that it monitors all async queues. The default thresholds were lowered to 100,000 per queue and the event severity was lowered to "minor" for all queues except "Internal". Dynamic Applications can now be aligned to Database Server, Data Collector, and Message Collector appliances. (Case: 00208680) (Jira ID: EM-47065)

Inbound Messaging

- Made updates to ensure that SNMP trap OID translation works as intended. (Case: 00415585) (Jira ID: EM-63204)

Logging

- Addressed an issue where log files from the **SL1 Developer Logs** page (System > Tools > SL1 Developer Logs) did not include debug logs in the report. (Case: 00353242) (Jira ID: SLUI-18789)
- Updated system_status.sh to prevent false alerts for MariaDB slow query logging. (Case: 00407869) (Jira IDs: EM-46396, EM-62548)

Monitoring Policies

- Updated web content monitoring to remove null bytes from the content before saving it in the database and checking it for matching expressions. (Case: 00390961) (Jira ID: EM-61807)
- When you set a sub-template for a Log Monitoring Policy in a Device Template, it will no longer have a prefix of "Test:" prepended to its name. (Case: 00414429) (Jira ID: EM-63095)

PowerPacks

- The "Support: Slow Query Check" Dynamic Application is now deprecated and disabled by default in the "ScienceLogic Support Pack" PowerPack. (Case: 00236431) (Jira ID: EM-49330)

Run Book Automations

- Resolved an issue where, if you disabled a user-initiated action, it would still appear in the **Tools** widget and the **Event Console** modal on the **Events Investigator** page. Similarly, addressed an issue in which Run Book Automation policies that had been changed from user-initiated to scheduled were not appearing on the **Automation Policy Manager** page (Registry > Run Book > Automation). (Case: 00411150) (Jira ID: SLUI-19024)

Schedule Management

- SL1 schedules for devices and device groups that have the same end times no longer result in a device remaining in maintenance beyond the end time. (Case: 00321089) (Jira ID: EM-56165)
- Devices will no longer exit maintenance mode when belonging to a maintenance window comprising two sequential device schedules. (Case: 00258995) (Jira ID: EM-51742)
- Managed schedules are now loaded in batches of 1,000 by default to prevent the Process Manager from becoming overloaded and stopping the scheduled jobs prematurely. Previously, all scheduled jobs were loaded simultaneously. You can update the default batch number of scheduled jobs by going to the **Database Tool** page (System > Tools > DB Tool) and entering the following in the ***SQL Query*** field, replacing `<batch number>` with the number of scheduled jobs you want to load per batch:

```
INSERT INTO master.system_custom_config (field,field_value) VALUES
('load_schedules_in_batches', <batch_number>) ON DUPLICATE KEY UPDATE
field = 'load_schedules_in_batches', field_value = <batch_number>
```

  (Case: 00225551) (Jira IDs: EM-48613, EM-48879)

Subscription Billing

- The billing process now ensures that data delivery to ScienceLogic generates proper billing. (Case: 00415301) (Jira ID: PTEL-1795)
- Collector groups (CUGs) that currently have no aligned Data Collectors will be converted to virtual CUGs upon upgrading to SL1 12.2.1.2 to ensure they are treated as non-billable as intended. This addresses an issue that was causing CUGs that were created in the default user interface (AP2) but had no aligned Data Collectors to be treated as non-virtual CUGs. (Jira ID: EM-64186)

Topology

- The topology crunch process now saves Layer 2 multi relationships in batches of 1,000 by default rather than all at once to prevent the system from overloading and stopping prematurely. (Case: 00386334) (Jira ID: EM-61675)

Recently Deprecated Features

12.2.0

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

> **NOTE:** If you are upgrading from a previous version of SL1, the 12.2.1.1 upgrade will not remove any existing PowerPacks. The PowerPacks listed below are still available for download from the PowerPacks Support page.

- Google Base Pack

12.1.0

- The 12.1.0 release deprecates the following PowerPacks and removes them from the ISO:

> **NOTE:** If you are upgrading from a previous version of SL1, the 12.2.1.1 upgrade will not remove any existing PowerPacks. The PowerPacks listed below are still available for download from the PowerPacks Support page.

  - 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

- In addition to the PowerPacks listed above, the "VMware: vSphere Base Pack" PowerPack has been removed from the 12.2.1.1 ISO due to a ***known issue***. It is still available for SL1 systems that upgrade to 12.2.1.1 from an earlier release.
- 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

Installing and Upgrading SL1

IMPORTANT: If you are upgrading from a release of SL1 prior to 12.2.1.x, you cannot upgrade to 12.2.1.1; you must download and upgrade to the upcoming 12.2.1.2 release. You can only consume SL1 12.2.1.1 if you are performing a fresh installation of SL1.

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

For detailed instructions on performing a new installation of SL1, see the ***Installation and Initial Configuration*** manual.

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

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

SL1 Extended Architecture

New installations of SL1 Extended Architecture are available only on SaaS deployments.

Important Installation Notes for SL1 Hollywood 12.2.1.1

This section includes important notes for installing the Hollywood 12.2.1.1 release.

CAUTION: ScienceLogic strongly recommends that you review these notes in their entirety before installing version 12.2.1.1.

Supported Upgrade Paths

There are no supported upgrade paths to SL1 12.2.1.1. This release is intended only for fresh installations of SL1.

If you are upgrading, you must download and consume the upcoming 12.2.1.2 release.

MariaDB

MariaDB version 10.4.31 is required for SL1 version 12.2.1.1.

Adjusting Maximum User Sessions

The SL1 12.1.1 release set the maximum number of simultaneous user sessions to 300. With this change, some users have received an "HTTP Response code was 429 (Too Many Requests)" error in SL1. If you receive this error, you can adjust the USER_MAX_SESSIONS value in **/opt/em7/nextui/nextui.conf** to increase the maximum value. To do so:

1. SSH into the SL1 appliance and log in as user **em7admin**.
2. At the command line, open the **nextui.conf** file in the vi editor:

```
sudo vi /opt/em7/nextui/nextui.conf
```

3. In the NextUI configuration file, set a new value for USER_MAX_SESSIONS, such as `USER_MAX_SESSIONS=1000` for 1,000 concurrent user sessions.
4. Save your changes and restart the NextUI service:

```
sudo systemctl restart nextui
```

For more information, see: https://support.sciencelogic.com/s/article/12971.

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.

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. Beginning with the Q4 2024 release, any custom Python 2 code that you have written for SL1 must be made compatible with Python 3, or it will cease to work properly.

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

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.

LDAP Authentication

This section describes the various LDAP authentication configurations that are supported in SL1.

CAUTION: If you are using an LDAP configuration other than one that is listed below, you should contact ScienceLogic Support or your Customer Success Manager to explain your use case. Non-supported configurations will be deprecated in a future release.

Configuration 1: Basic LDAP Authentication

- Configure an authentication profile that lists *EM7 Login Page* as the aligned credential source.
- The aligned authentication resource is associated with an LDAP/AD credential.
- It does not matter if the aligned LDAP/AD credential uses the %u or %e variables in its RDN string or if the RDN string is a defined value. If it is a defined value, it must also include a bind password.
- Optionally, an SSL certificate has been imported and installed if you are using LDAP over SSL.

NOTE: You can log in through REST API using an LDAP configuration.

Configuration 2: LDAP Configuration for CAC Authentication

- Configure one authentication profile, for most uses:
  - The authentication profile lists *CAC/Client Cert* as the aligned credential source.
  - The aligned authentication resource is associated with an LDAP/AD credential.
  - The aligned LDAP/AD credential uses a defined RDN string with a bind password; it cannot use the %u or %e variables in its RDN string.
- Configure a second authentication profile for administrator or maintenance access:
  - The authentication profile lists *EM7 Login Page* as the aligned credential source.
  - The aligned authentication resource is the *EM7 Internal* resource.

NOTE: You cannot log in through REST API using CAC authentication.

NOTE: You cannot have both CAC and non-CAC LDAP users on the same SL1 system.

NOTE: To disable a user's CAC authentication access, remove the user from the LDAP/AD server.

Configuration 3: Multiple LDAP Authentication Resources Used in the Same Authentication Profile

- Configure an authentication profile that lists *EM7 Login Page* as the aligned credential source.
- The authentication profile lists multiple aligned authentication resources, all of which are associated with LDAP/AD credentials.
- It does not matter if the aligned LDAP/AD credentials use the %u or %e variables in their RDN strings or if the RDN strings are a defined value. If they are defined values, they must also include bind passwords.
- Optionally, an SSL certificate has been imported and installed if you are using LDAP over SSL.

Configuration 4: One LDAP Authentication Resource Used in Multiple Authentication Profiles

- Configure one authentication profile:
  - The authentication profile lists *EM7 Login Page* as the aligned credential source.
  - The aligned authentication resource is associated with an LDAP/AD credential.
  - It does not matter if the aligned LDAP/AD credential uses the %u or %e variables in its RDN string or if the RDN string is a defined value. If it is a defined value, it must also include a bind password.
  - Optionally, an SSL certificate has been imported and installed if you are using LDAP over SSL.
- Configure a second authentication profile:
  - The authentication profile lists *EM7 Login Page* as the aligned credential source.
  - The aligned authentication resource is same one used in the first authentication profile.

Configuration 5: Basic HTTP Authentication with LDAP

- Configure an authentication profile that lists *HTTP Auth* as the aligned credential source.
- The aligned authentication resource is associated with an LDAP/AD credential.
- It does not matter if the aligned LDAP/AD credential uses the %u or %e variables in its RDN string or if the RDN string is a defined value. If it is a defined value, it must also include a bind password.
- Optionally, an SSL certificate has been imported and installed if you are using LDAP over SSL.

Known Issues for SL1 Hollywood 12.2.1.1

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 12.2.1.1:

- For this release, STIG-compliant configurations are available only for ISO installations; STIG-compliant upgrades are not available. When deploying a STIG-compliant configuration—also known as a military unique deployment (MUD) configuration—port 7700, the Web Configuration Utility, and the **Database Tool** page are all disabled. In addition, concurrent PowerShell, concurrent SNMP, and concurrent network interface collection are not supported for these deployments. (Jira IDs: EM-63763, EM-61841, EM-61842)
- A known issue is causing the directory `/var/lib/em7/update/patch_hook/.rpmdb` to be missing from ISO systems. For more information, including a resolution for this issue, see: https://support.sciencelogic.com/s/article/13541. (Jira ID: EM-63105)
- In ISO installations of SL1 12.2.1.1, a known issue is preventing AP2 objects from being included in PowerPacks for export. This issue will be addressed in an AP2 release in the near future. If you experience this issue prior to that release, you can work around the issue by dropping the master_ap2_public_views database and recreating it by running a SQL script on the Data Engine or All-In-One Appliance. You can obtain this script by contacting ScienceLogic Support. (Jira ID: SLUI-19623)
- 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)
- 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 SL1 12.2.1.1, 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 ID: EM-59277)
- 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)
- 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.

- The SL1 12.1.1 release set the maximum number of simultaneous user sessions to 300. With this change, some users have received an "HTTP Response code was 429 (Too Many Requests)" error in SL1. For more information about this error, see the section on ***Adjusting Maximum User Sessions*** and https://support.sciencelogic.com/s/article/12971.
- In new installations of SL1 12.2.1.1, 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 12.2.1.1 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 12.2.1.1 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)

- When creating a template from a Business Service, you might receive an error if the number of constituents and maximum constituents are greater than the maximum number of policies, which has a default value of 100. To work around this issue, you must increase the maximum number of policies using a GraphQL mutation, replacing `<increased value>` with a larger numerical value such as "1000":

```
mutation updateMaxValue{

  updateFeatureToggle(id: "system:BUSINESS_SERVICES_MAX_POLICIES",
  value: "<increased value>") {

    id

    value

  }

}
```

  (Jira ID: SLUI-19654)

- When editing information about a collector group using the **Collector Groups** page (Manage > Collector Groups), when you click **[Save]**, SL1 might remove information about any Data Collectors aligned to that collector group, even if you did not make any such changes. To work around this issue, you can instead make changes to collector groups using the **Collector Group Management** page (System > Settings > Collector Groups). (Jira ID: SLUI-19657)
- 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)
- The **[Set as Home Page]** button on the **Dashboards** page is disabled for newly created dashboards and existing dashboards that were imported. (Jira ID: SLUI-19539)
- SSH/Key credential tests do not work in STIG-compliant configurations. (Jira ID: EM-64250)

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