ScienceLogic

SL1 Hollywood 12.2.0 Release Notes

SL1 version 12.2.0 (Document revision 6)

SL1 Hollywood 12.2.0 Release Notes

> IMPORTANT: ScienceLogic strongly recommends that you review the ***installation and upgrade instructions***, important notes about ***upgrading*** SL1, and ***known issues*** for this release before installing or upgrading to SL1 12.2.0.

The SL1 Hollywood 12.2.0 release includes a number of important new features and enhancements:

- Totally revamped versions of the ***Device Investigator***, ***Event Investigator***, and ***Service Investigator*** pages that utilize Zebrium's AI/ML-driven root cause analysis insights
- A new ***Home dashboard*** that provides an at-a-glance insight into your IT estate
- Numerous ***user interface updates*** to provide a more unified and intuitive user experience
- A redesigned page for ***device configurations*** that displays the changes between two historical snapshots of a Dynamic Application
- The ability for some Extended Architecture users to ***deploy without Scylla***
- Plus ***many additional updates***

> IMPORTANT: As of version 12.2.0, SL1 no longer supports deployment on Oracle Linux 7 (OL7). Users who are upgrading from a version of SL1 prior to 12.1.1 that runs on OL7 ***must*** first upgrade to 12.1.1 and then convert to OL8 before they can upgrade to 12.2.0. For more information, see the ***Deployment*** section.

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

This document covers the following topics:

New Features and Enhancements in SL1 Hollywood 12.2.0

This section describes the features and enhancements that are included in SL1 Hollywood 12.2.0.

Business Services

- **What's new:** ***A new Service Investigator page*.** The **Service Investigator** page has been redesigned to consolidate service information in a single pane and provide additional context and value to users. This redesigned page also includes several components that integrate with Zebrium that display machine learning-generated log insights and root cause events.

  This new version of the **Service Investigator** page is designed to address incident management and service restoration use cases by correlating information from various sources into the context of a service. This allows you to quickly focus your investigation on the most likely cause of a service's health, availability, and risk scores and restore the service to a healthy state within a short time window.

  NOTE: The new **Service Investigator** page is disabled by default in SL1 12.2.0. To enable this new page, follow the instructions in the ***Using the New Service Investigator*** section of these release notes.

  The following updates were made to support this enhancement:

  - The **Health**, **Availability**, **Risk**, and **Anomalies** widgets were merged into new, single, consolidated pane on the **Service Investigator** page. This pane has the following tabs:
    - The **[Events]** tab, which displays a list of events for the chosen service or device.
    - The **[Changes]** tab, which displays a list of events that are created when PowerFlow pulls change data from ServiceNow or Restorepoint, is now enabled by default.
    - The **[RCA]** (Root Cause Analysis) tab, which indicates what is causing a device or service to be unhealthy based on the **Status Policy**.
    - The **[Log Insights]** tab, which displays a list of Zebrium events.
    - The **[Metric Anomalies]** tab, which was previously labeled **Anomalies** and displays a list of all devices within the selected services that have anomaly detection enabled.
  - A new information bar at the top of the **Service Investigator** page displays organization and system information such as ***Contact Organization***, ***Visible Organization***, and ***Owner***. This information bar also displays a preview of the sunburst chart, which you can click to see a more detailed breakdown of the **Health**, **Availability**, and **Risk** statuses of your devices.

    - The page also now includes a **Timeline** widget, which displays swim lanes (visual flowcharts that show a process from start to finish for an event) and bar graphs to show **Historical**, **Change**, **Health**, **Availability**, **Risk**, and **Zebrium** events. You can select any time range on the graph to display the **Changes**, **Health**, **Availability**, and **Risk** information specific to your chosen device or service in that selected time range.

- **For more information:** See *Using the Enhanced Service Investigator*.

Additional Business Services Updates

- Added a ***Status*** column to the **Business Services** page that indicates if a service is *Enabled* or *Disabled*. You can change the status of your services by clicking the **[Actions]** button (⋮) for the service and selecting either *Enable* or *Disable*.
- Whenever a business service registers a ServiceNow emergency change request, proposed change request, or disabled polling request, SL1 will now send a ServiceNow change request event to PowerFlow with the appropriate external reference information.

Dashboards

- **What's new:** ***A new Home dashboard.*** This release introduces a new **Home** dashboard, which serves as the default landing page for users who have not specified a different preferred landing page. This dashboard provides an at-a-glance insight into the current status for the IT estate of that user, including a list of recent events, total events by severity type, devices that currently have a "critical" or "major" status, and more.
- **For more information:** See *Home Dashboard*.

Additional Dashboards Updates

- Added a filter funnel icon to widgets on the **Dashboards** page. This icon allows you to view and select filters you can apply to the data that appears in the widget, similar to what you can do using the existing **Advanced Editor** filter options on the **Edit Widget** page. The widget header indicates the number of filters applied to the widget.
- You can now edit widget titles on the **Dashboards** page when you click the **[Edit]** button.
- Added a new *Severity Counts* visualization option for **Events** widgets that appear on the **Dashboards** page. This visualization option displays the number of severities in events by severity level; it does not require a selection in the ***Metrics & Properties*** drop-down field. When you click an event severity chip in this widget, you are redirected to the **Events** page with the appropriate event severity filter applied.
- You can now specify the number of decimal places that you want to display in *Number*, *Table*, and *Leaderboard* widget metric visualizations using the new ***Limit Decimal Precision*** field.

Deployment

- **What's new: *Oracle Linux 7 deployment is no longer supported*.** As of version 12.2.0, 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.

CAUTION: All customers who are upgrading from a version of SL1 prior to 12.1.1 that runs on OL7 ***must*** first upgrade to SL1 12.1.1 and then convert to OL8 before upgrading to SL1 12.2.0. 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 more information:** See the *Upgrade Notes* in these release notes as well as 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.

Device Management

- **What's new: *Zebrium integration for devices*.** When viewing details about a device, the **[Investigator]** and **[Events]** tabs now include several components that integrate with Zebrium and utilize its machine learning capabilities. The following updates were made to support this new feature:
  - You can now view Zebrium events on the **[Events]** tab, including suggestions, custom alerts, and accepted alerts. You can also filter the contents of the tab to view only Zebrium events.
  - A new banner at the top of the **[Investigator]** tab indicates if the selected device has Zebrium suggestions, custom alerts, or accepted alerts. You can click the **[VIEW]** link on the banner to go to the **[Events]** tab for that device, where you can review the Zebrium content.
  - **For more information**: See *Using the Device Investigator*.

- **What's new:** ***Dynamic Application snapshots and comparisons.*** The **[Configs]** tab of the **Device Investigator** has been redesigned to display more information about a specific Dynamic Application that is aligned to a given device and see all changes between two snapshots of that Dynamic Application.

  The following updates were made to support this new feature:

  - When you select a Dynamic Application from the collapsible pane on the left side of this page, you can click the **[View <*Dynamic Application Name*>]** button to open the **Dynamic Application Properties Editor** modal for that Dynamic Application.
  - You can choose two specific snapshot reference points and then compare the differences between the two. When you do so, all changes are highlighted. You can then click the **[Show <*X*> Changes]** button (where <*X*> is dynamically replaced with the number of changes) to view a modal that includes a more detailed breakdown of how the values changed between the two snapshots.
  - **For more information:** See *Viewing Device Snapshot Data*.

Additional Device Management Updates

- The **Device Overview** widget now displays at full width on the **Device Investigator** to ensure that all content is displayed correctly in the widget.

Events

- **What's new:** ***A new Event Investigator page***. The **Event Investigator** page has been redesigned to present critical data about a specific event in a clearer and more concise manner. Among other new features, this updated page includes a widget that provides machine learning-generated root cause information for Zebrium events. As part of this redesign, several widgets were added or updated on the page:
    - The new **Event Overview** widget appears at the top of the page and displays basic information about the event, including its message, severity, source, detection times, and occurrence count, as well as the name and organization of the impacted device. This widget also includes the **[Acknowledge]**, **[Clear]**, and **[View Automation Actions]** buttons that were on previous versions of the page.
    - The **Masked Events** widget was moved higher on the page to give it more prominence.
    - The new **Event Policy Information** widget displays information such as the name and description of the event policy that triggered the event, as well as its probable cause and potential resolution. From this widget, you can also click the **[View Event Policy]** button to view the full event policy.
    - The new **Device Details** widget displays information about the impacted device, such as its name, IP address, device ID, device class and category, number of active events, and more. You can also click a **[View Device]** button to view the **Device Investigator** page for the impacted device.
    - The new **Zebrium Root Cause Summary** widget, which displays for events with a Zebrium event source, includes root cause information, a word cloud that displays relevant words relating to the event, a list of other devices impacted by the same event, and a log of messages relating to the event. The widget also includes a **[View Full Root Cause Report in Zebrium]** button that you can click to open the root cause report in Zebrium in a new browser tab.
    - The **Logs** and **Note** widgets were renamed **Device Logs** and **Event Note**, respectively
    - **For more information:** See *Using the Event Investigator*.

Additional Events Updates

- In addition to the new **Zebrium Root Cause Summary** widget that appears in the **Event Investigator** for Zebrium events, the following updates were made to support integration of Zebrium events in SL1:
    - When creating or editing event policies, *Zebrium* now appears as an option under the ***Event Source*** drop-down field.
    - Zebrium options were added to the ***Event Type*** column on the **Events** page for any events that correspond with the Root Cause Report (RCR). There are now three valid Zebrium event types available: "Zebrium - Suggestion", "Zebrium - Accepted", and "Zebrium - Custom".
    - A new "Zebrium Event Policies" PowerPack contains event policies that are required for changing Zebrium alerts into SL1 events.

- Made the following updates to the **Event Insights** page (Events > Event Insights):
  - You can now filter the list to display event insights for one or more specific organizations using the new filter funnel icon at the top of the page.
  - Added a mouse-over feature to the "Top 10 Devices by Events Created" and "Top 10 Event Policies by Events Created" bar graph widgets, located in the "Tuning Targets" section of the page. This mouse-over feature allows you to hover your mouse over different points in the graph to view the number of events created for each severity as well as the total event count for each device and event policy, respectively.
- Added a new **Classic Events** option on the Advanced Menu under the "Events" heading. This option takes you to a refreshed version of the classic **Event Console** page, now presented in the default user interface.

Platform and Security

- **What's new:** ***Scylla is now optional on the Extended Architecture*****.** Users who are deployed on the SL1 Extended Architecture now have the option to remove existing Scylla databases from their Storage Nodes or to not deploy them in the first place if they do not require the machine learning-based anomaly detection service. This serves to lower resource utilization and cost. These users can then opt to delete any existing storage nodes from which Scylla has been removed. For more information, contact ScienceLogic Support.
- **For more information:** See *Disabling Scylla*.

Additional Platform and Security Updates

- SL1 version 12.2.0 includes multiple package updates to improve security and system performance.
- SL1 version 12.2.0 includes an upgrade to Kubernetes 1.27 for AWS deployments and Kubernetes 1.26 for on-premises deployments.
- After initially deploying or upgrading SL1 to version 12.2.0 or later, if you attempt to log in using the default system password, you will be required to create a new password.
- The use of HTTPS is now enforced by default. As a result, the ***Force Secure HTTPS*** checkbox was removed from the **Behavior Settings** page (System > Settings > Behavior).
- The Enterprise Key Management Service (EKMS) is now enabled by default to provide stronger encryption and security for user credentials.
- Most 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.

SL1 Studio

- **What's new: *Easier onboarding of new technologies*.** SL1 12.2.0 is compatible with the new SL1 Studio lineup of low-code/no-code toolkits, which are designed to help you extend SL1's existing capabilities and monitor technologies for which no generally available PowerPacks or integrations currently exist. The SL1 Studio includes the following toolkits:
  - CLI: Toolkit
  - Prometheus Toolkit
  - REST: Toolkit
  - Dynamic Application Builder
  - PowerPack Quality Assessment Tool
  - PowerFlow Software Developer Kit
- **For more information:** See the ***SL1 Studio*** page on the Support portal.

User Interface

- **What's new: *A unified user experience*.** Many pages throughout the default user interface were redesigned to make them more intuitive and visually appealing for users, resulting in a more modern and unified user experience.

Additional User Interface Updates

- Added a home icon at the top of the left navigation bar. By default, clicking this icon displays the ***new Home dashboard***. To change your home page, navigate to any page in SL1, click your user name drop-down in the top right corner of the page, and then select *Set as Home Page*.
- Updated the feature that automatically logs users out of SL1 after the period of inactivity that is specified in the ***User Login Session Timeout*** setting on the **Behavior Settings** page (System > Settings > Behavior). Now, a prompt warning users that they are going to be logged out due to inactivity appears with a countdown one minute before the session times out. Any interaction with SL1, such as moving the mouse or pressing a key, will dismiss the warning and refresh the timeout clock.
- If you apply a transitional theme with a custom logo in the default SL1 user interface, that logo will now persist if you navigate to the classic user interface.

Additional New Features and Enhancements in SL1 Hollywood 12.2.0

Agent

- The agent pipeline no longer requires the Scylla database. (For more information about this change and the conditions under which you can remove existing Scylla databases, see the *Platform* section.) As part of this change, the agent pipeline now consumes and summarizes 1-minute and 5-minute data payloads without the need for Scylla. When collecting data in intervals greater than 1 minute, new Streamer check-in calls on the pipeline to prevent the agent from appearing unavailable and return more detailed responses regarding the upload.
- A new ***Require TLS Validation for Gen 0 Agent*** checkbox was added to the **Behavior Settings** page (System > Settings > Behavior). When this checkbox is selected, Gen 0 agents that operate outside of the Extended Architecture will require TLS validation to upload data.

> **NOTE:** To enable this validation, all Data Collectors and Message Collectors that will ingest agent data must have a valid and signed TLS certificate.

- Updated the agent responder so that attempts to align Windows PowerShell Dynamic Applications to non-Windows agents should no longer cause polled data to be pushed to the agent erroneously.
- The Windows agent now attempts to exclude desktop per-user login Windows sessions from the list of current Windows services.
- Updated the SiloAgent.exe --diag file to save all data in the datakeep folder, not just the most recent data.
- SL1 12.2.0 includes updates to improve agent security and performance.

Anomaly Detection

- Added a new potential status to the **Machine Learning** page. With this update, if anomaly detection for a metric lacks sufficient data, either because detection needs at least one day of monitoring or the data for that metric is irregular, the status "Waiting for Data" appears in the ***Anomaly Detection*** column. When SL1 has enough data to train a high-quality anomaly detection model, the device or metric is automatically re-queued.
- Made improvements to the speed and accuracy of machine learning-based anomaly predictions.

Data Collection

- Updated data pull to ignore storage objects that have not yet been converted to Python 3.

GraphQL

- Made the following GraphQL updates to support Zebrium service connections and integrations with devices, events, and services:
    - The "deploymentId" field is no longer required in Zebrium service connections.
    - Added four new mutations that use the supplied endpoint and credentials to create an API call that finds the value in the "deploymentId" field in Zebrium connection services and adds it to the configuration. This API call also verifies that both the endpoints and access tokens can make authenticated calls to the Zebrium API. These four mutations are:
        - createServiceConnection
        - updateServiceConnection
        - createZebriumConnection
        - updateZebriumConnection
    - Added new event-related fields to the "logAlert" type, which is returned by the "logAlertBuckets" query. Among these fields is "relatedEvents". When you query for log alerts by event IDs, this field will return details about related events and their aligned devices, allowing you to see which devices are impacted by the issues identified in the Root Cause Analysis report.
    - Added a new "logAlertCandidates" query that polls for Zebrium log alerts, as well as a new "alertCreatedTimestamp" field on queries that return the "logAlert" type to report the time the Zebrium alert was created.
- Made the following GraphQL updates to support updates to machine learning-based anomaly detection:
    - Added a more efficient field, "aiMachineLearningMetricAnomalies", to device and devices queries. This field replace queries using the "machineLearningPolicy" field with a more flexible set of fields.
    - Queries for "anomalyIndexThresholds" and "updateAnomalyIndexThresholds" now return an error message when anomaly detection is disabled, similar to the behavior of other anomaly detection queries.
- Added a "systeminformation" query that returns the current SL1 Classic (EM7) version number in the field "em7Version".
- Added the "userLoginSessionTimeout" field to the "systemSettings" query.

PowerFlow

- SL1 12.2.0 is compatible with ***PowerFlow 2.7.0***.

PowerPacks

- The 12.2.0 ISO includes the following updated PowerPacks:
  - *Entity MIB v101*
  - *Generic Switch/Router MIB Support v104*
  - *Host Resource Core v108*
  - *Host Resource Processes v101*
  - *Juniper Base Pack v103*
  - *Linux Base Pack v110*
  - *Net-SNMP Base Pack v102*
  - *Supplemental Device Class Pack v104*

Snippet Framework

- When creating or editing a Dynamic Application in SL1, there are two new options available in the ***Application Type*** field: *Snippet Framework Performance* and *Snippet Framework Configuration*. These options are now also reflected in the *Type* column on the **Dynamic Applications Manager** page (System > Manage > Dynamic Applications).
- Updated the **[Collections]** tab of the **Device Investigator** to display Snippet Framework Dynamic Application types in the *Type* column.
- Made the following updates to improve the speed and efficiency of Snippet Framework Dynamic Applications:
  - Updated the SL1 collectors to run Snippet Framework Dynamic Application jobs as a subprocess, which allows for quicker and more cache-aware jobs.
  - Added the ability to change the number of processes that the Snippet Framework Dynamic Application type's process pool can run simultaneously, as well the timeout value for each process. These limits are set in `silo.conf`. If the limits are not set, the default values are 2 simultaneous processes and 15 minutes before timing out.
  - Added a device limit for the Snippet Framework scheduler that allows you to change the number of devices that a WorkOrder can run simultaneously. This device limit is set in `silo.conf`. If the limit is not set, it has a default value of 100.

System Update

- A new pre-upgrade check was added to prevent you from upgrading to 12.2.x and above if your SL1 stack contains appliances with multiple operating systems. This ensures that all of your SL1 appliances are running on Oracle Linux 8.

- Updated deployment log messages relating to license expiration, disk/partition free space, internet connectivity, and more to provide additional details about why a pre-upgrade failure might be occurring. This helps catch potential upgrade problems before you begin the upgrade, shortens upgrade time, and allows for easier recovery should an issue occur during upgrade.
- A new "SL1: System Upgrade Assessment" PowerPack was added to the 12.2.0 ISO. This PowerPack, which requires no manual configuration, includes a Run Book Automation policy that detects any Execution Environments that are utilizing Python 2 and generates a major event and an admin notification if any Python 2 elements are detected on your SL1 system. This automation runs every two weeks initially, but more frequently over time.

Topology

- Added a new option for CDP topology collection that can be activated in the `cdp_device_name_search` column on the `master.system_settings_core` database table.
- Updated topology crunch processes to check whether the `master_dev.topo_override` table exists in the database and, if so, which records topology crunch can modify.

Issues Addressed in SL1 Hollywood 12.2.0

This section describes the issues that were addressed in SL1 Hollywood 12.2.0.

Agent

- Addressed an issue with AIX agent performance data collection. (Case: 00340755) (Jira ID: EM-57987)

API

- Event suppressions configured for device groups now properly delete via the ScienceLogic API. (Case: 00260994) (Jira ID: EM-51735)
- Addressed an issue in the ScienceLogic API that was removing credentials' aligned organizations in POST requests. (Cases: 00246521, 00353128) (Jira ID: EM-49696)

Dashboards

- You can now generate a PDF of a dashboard that will print on a single page. (Case: 00285110) (Jira ID: SLUI-17922)
- Resolved issues that were causing dashboard widgets with *Table* visualizations to not display columns in the selected order nor with the correct defined values. (Case: 00321131) (Jira ID: EM-56310)
- You can now have a fixed selection state on Interfaces widgets with *Table* visualizations if your account belongs to an organization for which a Network Interface's emissary is set. (Case: 00304015) (Jira ID: EM-55112)

Data Collection

- Addressed an issue that was causing the critical ping feature to not work due to an unhandled exception. (Case: 00403316) (Jira ID: EM-62436)
- Updated SNMPv3 data collection to ensure that it performs as expected when the Concurrent SNMP Service is enabled. (Case: 00318853) (Jira ID: EM-56917)
- Added an option to disable Kerberos-based WinRM message encryption if error messages appear after upgrading to the pyKerberos package. (Case: 00344683) (Jira ID: EM-58320)

Deployment

- Addressed an issue to ensure that auto licensing works as intended on cloud-based deployments of SL1. (Cases: 00355245, 00373343) (Jira ID: EM-58701)
- Resolved an issue with AWS AMI deployment to ensure it completes initial installation. (Case: 00370727) (Jira ID: EM-60411)

Device Management

- Addressed an issue that was resulting in duplicate interface names. (Cases: 00172374, 00317971) (Jira ID: EM-44532)
- SL1 now generates an alert indicating whenever a device is not removed from scheduled maintenance mode as expected. (Cases: 00307558, 00327215) (Jira ID: EM-55409)
- Resolved an issue to ensure that the correct user ID displays to indicate which user edited a device interface. (Case: 00153769) (Jira ID: EM-42097)
- The ***Subnet Mask*** field now accepts integers 0-128 to allow for IPv6 IP address prefixes. (Case: 00199461) (Jira ID: EM-46118)

Documentation

- Added a new section in the ***System Administration*** manual detailing ***SL1's self-monitoring*** capabilities. (Case: 00376158) (Jira ID: EM-61098)
- Added a new section to the ***System Administration*** manual to address known limitations with ***collector group load balancing and device state***. (Case: 00372890) (Jira ID: EM-61110)
- Updated the ***System Administration*** manual with instructions to confirm changes on the **Appliance Manager** page when ***updating an appliance's IP address***. (Case: 00386458) (Jira ID: EM-61615)
- Updated the ***Run Book Automations*** manual to clarify language relating to ***user-initiated automation policies***. (Case: 00380996) (Jira ID: EM-61239)
- Updated the ***Classic Maps*** manual to remove references to deprecated features. (Case: 00389014) (Jira ID: EM-61731)

Events

- Resolved an issue in which the **Events** page was displaying only events that had a severity of "Notice" after upgrading SL1. (Jira ID: SLUI-17984) (Case: 00365477)
- Resolved an issue that caused event suppressions to stop working with device groups after upgrading SL1. (Cases: 00376097, 00377769, 00379446) (Jira IDs: EM-60621, EM-61157)
- Addressed an issue that was causing unhandled exceptions to occur when using external RSS feeds to generate SL1 events. (Case: 00350806) (Jira ID: EM-59029)
- Added the ability to generate audit logs for event policy changes when an event policy is updated or deleted. (Case: 00336359) (Jira ID: EM-57561)
- Addressed an issue in which SL1 displayed a "failed to connect to database" error when users attempted to open event logs. (Case: 00341251) (Jira ID: EM-58220)

GraphQL

- Resolved an issue that was causing GQL queries to fail with a "read timed out" error at scale for the PowerFlow application "Sync Devices from SL1 to ServiceNow." (Cases: 00299817, 00391049) (Jira ID: EM-55501)

Inbound Messaging

- Resolved an issue that was causing SL1 to generate errors when non-ASCII characters were included in the file name of inbound email attachments. (Case: 00306059) (Jira ID: EM-55085)

Licensing

- Addressed an issue where the SL1 user interface was not accessible due to appliance license issues. (Cases: 00306955, 00347788) (Jira ID: EM-55049)

Monitoring Policies

- Resolved issues with web content monitoring policies that were preventing SL1 from properly storing and displaying content collected from monitored websites that use non-ASCII characters and encoding other than UTF-8. (Case: 00342279) (Jira ID: EM-58224)

PowerPack Management

- Made updates to ensure users can remove PowerPacks using the SL1 API. (Case: 00321268) (Jira IDs: SOL-23215, EM-56086)
- Addressed an issue where Dynamic Application threshold settings that were specified in device templates were not exporting or importing properly with their associated PowerPack. (Case: 00311202) (Jira IDs: SOL-23008, EM-55741)
- Addressed an issue that was preventing users from deleting PowerPacks that included PowerShell credentials. (Jira ID: EM-53453)

Reports

- Ensured that reports generated on SaaS SL1 instances reflect the correct data. (Cases: 00308648, 00379163) (Jira ID: EM-55956, EM-55468)

System Processes

- 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)

System Update

- Updated the Message of the Day (MOTD) to ensure that it displays the correct sudo command when users do not set a database password. (Case: 00311586) (Jira IDs: EM-55493, EM-55919)

User Interface

- Addressed an issue that was causing the SL1 user interface to be inaccessible due to an internal server error whenever the apuser database password included a special character. With this update, you can include the following approved special characters in the apuser database password: ! $ & ' ( ) * + , ; = (Case: 00375806) (Jira ID: SLUI-18149)
- Resolved an issue that was causing the page format to break when editing the **User Preferences** page (Registry > Account > User Accounts > User Preferences). Also with this update, hidden field values are no longer modified when editing user preferences on this page. (Cases: 00248436, 00362586) (Jira ID: EM-49484)

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 12.2.0 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 12.2.0 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 12.2.0 ISO due to a ***known issue***. It is still available for SL1 systems that upgrade to 12.2.0 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

11.2.0

- The Inbox feature is deprecated and is available only for reports in the classic user interface.
- The IPMI features were deprecated in SL1.
- The Knowledge Base and Knowledge Base tab were removed from SL1.
- The clipboard feature was removed from Ticketing. The access hook for the clipboard feature was also removed.

Installing and Upgrading 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.

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.

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

Important Upgrade Notes for SL1 Hollywood 12.2.0

This section includes important notes for upgrading existing SL1 systems to the Hollywood 12.2.0 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 12.2.0.

Supported Upgrade Paths

The SL1 12.1.1, 11.1.0, and 10.1.0 releases all included major updates that you must consume before you can upgrade to 12.2.0, if you have not done so already.

Therefore, depending on the version of SL1 that you are currently running, you might be required to upgrade to one or more earlier versions of SL1 before you can upgrade to 12.2.0.

CAUTION: All customers who are upgrading from a version of SL1 prior to 12.1.1 ***must*** first upgrade to SL1 12.1.1 and then convert to OL8 before upgrading to SL1 12.2.0. 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.

You can upgrade to SL1 12.2.0 using one of the following upgrade paths:

- *12.1.x to 12.2.0 and already on OL8*
- *12.1.x or 11.x to 12.2.0 but not yet on OL8*
- *10.x to 12.2.0*
- *8.x to 12.2.0*

See the sections below for additional details.

Upgrade Path 1: 12.1.x to 12.2.0 and already on OL8

If you are currently on SL1 12.1.x and are already running Oracle Linux 8 (OL8), you can *upgrade* directly to version 12.2.0.

After the SL1 upgrade, you must upgrade your SL1 appliances to MariaDB 10.4.31.

Upgrade Path 2: 11.x or 12.1.x to 12.2.0 but not yet on OL8

If you are currently running one of the following versions of SL1 and you want to convert your operating system to OL8, you must follow the steps outlined in this section:

- 12.1.x (running on OL7)
- 11.x

To upgrade your SL1 system and convert to OL8, you must complete the following tasks in order:

1. If you have not already done so, *download* and *import* version 12.1.0.2 to your SL1 system. Otherwise, if you are already running SL1 12.1.0.2, you can skip to step 2.

> **NOTE:** You do not need to stage or deploy the 12.1.0.2 update; you just need to import it. As part of this import process, you will need to pause for 30 minutes so the import process can import an RPM file.

2. *Download* the 12.1.1 patch file from the *ScienceLogic Support site*.
3. Import the SL1 12.1.1 update. To do so, you must do one of the following:
   - If you have already deployed SL1 12.1.0.2, you can *import* the 12.1.1 update from the **System Updates** page (System > Tools > Updates) in SL1. When the 12.1.1 patch has an ***Import Status*** of "Complete," proceed to step 8.
   - If you have not deployed SL1 12.1.0.2, you must import the 12.1.1 update using the command line interface. Proceed to step 4.
4. SSH in to your primary Database Server or All-in-One Appliance and ensure that you have at least 7GB of free space on the partition where the patch file will be uploaded.
5. Upload the patch file to your primary Database Server or All-in-One Appliance. Write down the file path of the patch file.
6. Use the following command to import the patch file on to your primary Database Server or All-in-One Appliance:

   ```
   siloupdate import-patch <file path to patch file>
   ```

   where you replace `<file path to patch file>` with the file path you wrote down in the previous step.

> **NOTE:** It will take several minutes for this command to complete.

7. When the command completes, log in to SL1 and go to the **System Updates** page (System > Tools > Updates). Confirm that the 12.1.1 patch is listed and that it has an ***Import Status*** of "Complete."

8. *Run the pre-upgrade check, put your appliances in maintenance mode, then stage and deploy* the SL1 12.1.1 update.

9. Upgrade your SL1 appliances to MariaDB 10.4.29.

> NOTE: If you were previously running SL1 12.1.0 or 12.1.0.2 and had already upgraded your SL1 appliances to MariaDB 10.4.29, you can skip this step.

10. Begin the OL8 operating system conversion. For more information, see the *OL8 Conversion Resource Center* on the ScienceLogic Support portal, which includes links to the Conversion Guide with full conversion steps.

> IMPORTANT: As part of this conversion, you will need to re-ISO your SL1 Database Server, Data Collectors, and Message Collectors. After you do so, they will be running on OL8 and MariaDB 10.4.28.

11. Upgrade to SL1 version 12.2.0.

12. Upgrade your SL1 appliances to MariaDB 10.4.31.

Upgrade Path 3: 10.x to 12.2.0

If you are currently running a version of SL1 10.x, you ***must*** first upgrade to the following releases prior to upgrading to 12.2.0, depending on your current version:

- 11.x, which included a conversion of all PHP code to PHP 7
- 12.1.0.2, which included changes to the siloupdate-manager service
- 12.1.1, which is a prerequisite for converting to Oracle Linux 8 (OL8)

You must then convert your SL1 operating system to OL8.

Therefore, if you are currently running version 10.x, then the upgrade to SL1 version 12.2.0 might require multiple maintenance windows:

1. *Upgrade* to SL1 version 11.x.
2. Upgrade to the *MariaDB version that corresponds to that SL1 release*.
3. Follow the steps in the section *11.x or 12.1.x to 12.2.0 but not yet on OL8*.

Before upgrading from SL1 10.x to 11.x, consult the appropriate 11.x *release notes* or contact ScienceLogic Support to confirm that the upgrade paths between those two versions is supported.

For additional information about the PHP conversion and its impact, see the section on *PHP Updates*.

Upgrade Path 4: 8.x to 12.2.0

If you are currently running a version of SL1 8.x, you ***must*** first upgrade to the following releases prior to upgrading to 12.2.0, depending on your current version:

- 8.12.x, which included a new system update tool
- 10.x, which included an upgrade from MariaDB 10.1 to MariaDB 10.4
- 11.x, which included a conversion of all PHP code to PHP 7
- 12.1.0.2, which included changes to the siloupdate-manager service
- 12.1.1, which is a prerequisite for converting to Oracle Linux 8 (OL8)

You must then convert your SL1 operating system to OL8.

Therefore, if you are currently running version 8.14.x or earlier, then the upgrade to SL1 version 12.2.0 might require multiple maintenance windows:

1. If you are on a version of SL1 prior to 8.12.x, ***upgrade*** to version 8.12.x. Otherwise, skip to step 3.
2. If you are upgrading to SL1 8.12.0, upgrade to the MariaDB version 10.1.38; if you are upgrading to SL1 8.12.1 or 8.12.2, upgrade to MariaDB 10.1.40.
3. Upgrade to SL1 version 10.x.
4. Upgrade to the ***MariaDB version that corresponds to that SL1 release***.
5. Upgrade to SL1 version 11.x.
6. Upgrade to the ***MariaDB version that corresponds to that SL1 release***.
7. Follow the steps in the section ***11.x or 12.1.x to 12.2.0 but not yet on OL8***.

Before upgrading between SL1 versions, consult the appropriate ***release notes*** or contact ScienceLogic Support to ensure that the upgrade paths between those versions are supported.

For additional important notes, see the section on ***Upgrading from Version 8.14.x or Earlier***.

For additional information about the PHP conversion and its impact, see the section on ***PHP Updates***.

Unsupported Upgrade Paths

Users who have not yet deployed or upgraded to an SL1 12.1.x version that is running on Oracle Linux 8 (OL8) cannot upgrade to SL1 12.2.0.

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?
12.2.0	10.4.31	Yes
12.1.1 (OL7)	10.4.29	Yes
12.1.1 (OL8)	10.4.28	Yes
12.1.0.2 Upgrade (OL7)	10.4.29	Yes
12.1.0.2 ISO (OL8)	10.4.28	N/A
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
11.2.4.1	10.4.28	Yes
11.2.4	10.4.28	Yes
11.2.3	10.4.28	Yes
11.2.2	10.4.26	Yes
11.2.0	10.4.24	Yes
11.1.6.1	10.4.28	Yes
11.1.6	10.4.28	Yes
11.1.5	10.4.26	Yes
11.1.4	10.4.26	Yes
11.1.3	10.4.25	Yes
11.1.2	10.4.24	Yes
11.1.1	10.4.22	Yes
11.1.0	10.4.20	Yes
10.2.7	10.4.27	Yes
10.2.6.1	10.4.26	Yes
10.2.6	10.4.26	Yes
10.2.5	10.4.22	Yes
10.2.4.1	10.4.22	Yes
10.2.4	10.4.22	Yes
10.2.3	10.4.21	Yes
10.2.2	10.4.18	Yes
10.2.1	10.4.18	Yes
10.2.0	10.4.18	Yes
10.1.8.1	10.4.21	Yes
10.1.8	10.4.21	No
10.1.7	10.4.18	No
10.1.6	10.4.18	Yes

SL1 Release	Required MariaDB Version	Requires Appliance Reboot?
10.1.5	10.4.12	Yes
10.1.4	10.4.12	Yes
10.1.3	10.4.12	Yes
10.1.2	10.4.12	No
10.1.1	10.4.12	Yes
10.1.0	10.4.12	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.

Using the New Service Investigator

SL1 version 12.2.0 introduces a fully revamped **Service Investigator** page. However, this update is disabled by default in 12.2.0.

You have the option to temporarily enable or disable the new **Service Investigator** page using GraphQL mutations or permanently enable or disable it through the `nextui.conf` file.

NOTE: If you have a Database Server and one or more Administration Portals in your SL1 system, then you must enable the new page on each appliance. Otherwise, the new page will appear only on the appliances that have the toggle enabled.

Enabling The Service Investigator Page

To ***temporarily*** enable the new **Service Investigator** page and the ServiceNow or RestorePoint swim lane diagrams on the new **Timeline** widget:

1. Access the GraphiQL interface by typing the URL or IP address for SL1 in a browser, add /gql to the end of the URL or IP address, and press Enter.
2. To temporarily enable the new **Service Investigator** page, type the following mutation in the main query pane:

```
mutation investigatorPage {
  updateFeatureToggle(id: "system:_AP2_BUSINESS_SERVICES_INVESTIGATOR",
value: "enabled") {
    id
    value
  }
}
```

3. To temporarily enable the ServiceNow swim lane diagrams on the new **Timeline** widget, type the following mutation:

```
mutation updateServiceNowSwimLane {
  updateFeatureToggle(id: "system:_AP2_BUSINESS_SERVICES_SERVICENOW",
value: "enabled") {
    id
    value
  }
}
```

4. To temporarily enable the RestorePoint swim lane diagrams on the new **Timeline** widget, type the following mutation:

```
mutation updateRestorePointSwimLane {
  updateFeatureToggle(id: "system:_AP2_BUSINESS_SERVICES_RESTOREPOINT",
value: "enabled") {
    id
    value
  }
}
```

NOTE: After you have enabled or disabled the new **Service Investigator** page via GraphQL mutations, you must refresh the page or sign out and sign back into your account. If the nextui service restarts, all GraphQL feature toggles will also need to be reset. To make these changes permanent, you can modify the `nextui.conf` file as outlined in the instructions below.

To ***permanently*** enable the new **Service Investigator** page and the ServiceNow or RestorePoint swim lane diagrams on the new **Timeline** widget:

1. Use SSH to access your SL1 appliance.
2. Using vi or another text editor, edit the `/opt/em7/nextui/nextui.conf` file. To do so, enter the following at the shell prompt:

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

3. Add the following line at the bottom of the `nextui.conf` file:

```
_AP2_BUSINESS_SERVICES_INVESTIGATOR=enabled
AP2_BUSINESS_SERVICES_SERVICENOW=enabled
AP2_BUSINESS_SERVICES_RESTOREPOINT=enabled
```

Disabling The Service Investigator Page

To ***temporarily*** disable the new **Service Investigator** page:

1. Access the GraphiQL interface by typing the URL or IP address for SL1 in a browser, add /gql to the end of the URL or IP address, and press Enter.
2. To temporarily disable the new **Service Investigator** page, type the following mutation in the main query pane:

```
mutation investigatorPage {
  updateFeatureToggle(id: "system:_AP2_BUSINESS_SERVICES_INVESTIGATOR",
value: "disabled") {
    id
    value
  }
}
```

3. To temporarily disable the ServiceNow swim lane diagrams on the new **Timeline** widget, type the following mutation:

```
mutation updateServiceNowSwimLane {
  updateFeatureToggle(id: "system:_AP2_BUSINESS_SERVICES_SERVICENOW",
value: "disabled") {
    id
    value
  }
}
```

4. To temporarily disable the RestorePoint swim lane diagrams on the new **Timeline** widget, type the following mutation:

```
mutation updateRestorePointSwimLane {
  updateFeatureToggle(id: "system:_AP2_BUSINESS_SERVICES_RESTOREPOINT",
value: "disabled") {
    id
    value
  }
}
```

NOTE: After you have enabled or disabled the new **Service Investigator** page via GraphQL mutations, you must refresh the page or sign out and sign back into your account. If the nextui service restarts, all GraphQL feature toggles will also need to be reset. To make these changes permanent, you can modify the `nextui.conf` file as outlined in the instructions below.

To ***permanently*** disable the new **Service Investigator** page and the ServiceNow or RestorePoint swim lane diagrams on the new **Timeline** widget:

1. Use SSH to access the SL1 appliance.
2. Using vi or another text editor, edit the `/opt/em7/nextui/nextui.conf` file. To do so, enter the following at the shell prompt:

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

3. Add the following line at the bottom of the `nextui.conf` file:

   ```
   _AP2_BUSINESS_SERVICES_INVESTIGATOR=disabled
   AP2_BUSINESS_SERVICES_SERVICENOW=disabled
   AP2_BUSINESS_SERVICES_RESTOREPOINT=disabled
   ```

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.

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 12.2.0, 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.

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.

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.

SSH Collector Removal

NOTE: This section applies to users who are upgrading from SL1 11.3.x or earlier. If you are upgrading from SL1 12.1.0 or later, you can ignore this section.

The SSH Collector container was removed from SL1 in version 12.1.0. To support this change, the "Data Collection: SSH Collector" process is no longer available in new installations of SL1 as of 12.1.0 or later.

If you are upgrading to 12.2.0 from an earlier release and you were previously using the SSH Collector, you must reboot any Data Collectors that were previously using the "Data Collection: SSH Collector" process. After upgrading SL1, you can go to the **Appliance Manager** page (System > Settings > Appliances) to determine which appliances might require a reboot.

Required PowerPack Updates

NOTE: This section applies to users who are upgrading from SL1 11.2.x or earlier. If you are upgrading from SL1 11.3.0 or later, you can ignore this section.

Required Version Updates

If you are using the following PowerPacks and you are upgrading from SL1 11.2.x or earlier, you must upgrade to the specified minimum supported versions before upgrading to SL1 version 12.2.0:

- Cisco: ACI v112
- Cisco: AppDynamics v102
- Cisco: Cloud Services Platform v107
- Cisco: Viptela v104
- Datacenter Advanced Enrichment Actions v106
- Dynatrace v105
- HTTP Action Type v103
- IBM: DB2 v104
- Kubernetes v104
- Linux: Base Pack v105
- Linux SSH Automation v104
- Microsoft: Azure v115
- Microsoft: Office 365 v106
- NetApp: Base Pack v106
- Oracle: MySQL v102

- VMware Automation v102
- Windows PowerShell Automation v104

Earlier versions of these PowerPacks will not prevent SL1 version 12.2.0 from installing or operating, but they might not operate as expected after the SL1 upgrade due to technical incompatibilities.

Required Credential Updates

Some PowerPacks require you to update their credentials before you upgrade to version 11.2.0 or later. Therefore, if you are using one of the following PowerPacks and are upgrading from a version of SL1 prior to 11.2.0, you must edit an HTTP header in the credential before you upgrade to version 12.2.0:

- Cisco: ACI Multisite
- CouchBase
- Dell: EMC VMAX
- Google: Cloud Platform
- LayerX: Appliance Monitoring
- ScienceLogic: PowerFlow
- PowerPacks built using the REST PowerPack

To edit the credential HTTP header:

1. Go to the **Credentials** page (Manage > Credentials).
2. Locate the credential you created, then click its **[Actions]** icon and select *Edit/Test*.
3. Find the "Content-Type: application/json" HTTP header, then remove the space in the HTTP header so that the new header reads "Content-Type:application/json".
4. Repeat step 3 for any other HTTP header entries in the credential.
5. Click **[Save & Close]**.
6. Repeat these steps for any other credential relating to the PowerPacks in the list above.

Required Updates for Users Running Amazon RDS (Aurora MySQL 5.7)

If you are using Amazon RDS (Aurora MySQL 5.7) with SL1 and are upgrading from a version of SL1 prior to 11.2.0, then you must update to the following PowerPack versions before installing SL1 version 12.2.0:

- Cisco: UC VOS Applications v110

Monitoring Windows with WMI

NOTE: This section applies to users who are upgrading from the following releases:

- SL1 11.1.0 through 11.1.2
- Any SL1 release prior to 10.2.5

If you are upgrading from the following releases, you can ignore this section:

- 11.2.0 and later
- 11.1.3 or a later 11.1.x version
- 10.2.5 or a later 10.2.x version

SL1 versions 11.2.0, 11.1.3, and 10.2.5 included a new WMI client in response to Microsoft security updates. This change enables WMI Dynamic Applications to collect data from hardened Windows servers, but also has a major impact on system scalability.

This change significantly decreases the number of Microsoft Windows servers that can be supported on each Data Collector in your SL1 system. Users who need to monitor Windows devices using WMI should analyze their system resources and capacity before upgrading to 12.2.0. For guidance about sizing, see the updated Collector Sizing guidelines for WMI endpoints.

To avoid this impact, ScienceLogic recommends using SNMP collection for two-core Windows servers and PowerShell collection for four-core Windows servers. For more information, see this Support Knowledge Base article.

Pre-Upgrade Test for PhoneHome Database Servers

NOTE: This section applies to users who are upgrading from SL1 11.1.x or earlier and have an existing PhoneHome configuration. If you are upgrading from SL1 11.2.0 or later or you do not have a pre-11.2.0 PhoneHome configuration, you can ignore this section.

SL1 version 11.2.0 included a new pre-upgrade test that checks for existing PhoneHome Database Servers.

This pre-upgrade test looks for PhoneHome token IDs inside the /home/phonehome0/config.json file and fails if the value of the token ID field is less than or equal to "0". In previous versions of SL1, the primary PhoneHome Database was not self-registered with a token, causing it to have an ID of "0".

Therefore, if you are upgrading from version 11.1.x or earlier and you have a PhoneHome configuration, then you must perform these one-time manual configuration steps on all Database Servers in your PhoneHome configuration prior to upgrading to SL1 version 12.2.0:

1. Log in to the console of the Database Server or use SSH to access the server.
2. To determine if all of your PhoneHome Database Servers are registered, type the following command and check if any have an ID value of "0":

   ```
   cat /home/phonehome0/config.json
   ```

3. If a PhoneHome Database Server has an ID value of "0", type the following command and locate the ID of the current appliance:

   ```
   phonehome status
   ```

4. Type the following command and locate the PhoneHome token:

```
phonehome token <ID from step 3>
```

5. Type the following command to register the PhoneHome token:

   ```
   phonehome register <token from step 4>
   ```

6. Repeat steps 3-5 for all PhoneHome Database Servers that have an ID value of "0".
7. Type the following command to ensure that all of your PhoneHome Database Servers are synced:

   ```
   phonehome sync
   ```

8. Repeat step 2 and confirm that all Database Servers have ID values greater than "0".

NOTE: Do not attempt to upgrade to 12.2.0 until all pre-upgrade tests are successful on all PhoneHome Database Servers.

IMPORTANT: The PhoneHome server process runs as an unprivileged user that will not be able to bind to a privileged port (1-1023). Therefore, when you choose a custom port, you must choose port 1024 or higher.

PHP Updates

NOTE: This section applies to users who are upgrading from SL1 10.2.x or earlier. If you are upgrading from SL1 11.1.0 or later, you can ignore this section.

In SL1 version 11.1.0, all PHP code was converted to PHP 7. Therefore, if you are upgrading from a version of SL1 prior to 11.1.0, please note the following:

- If you are upgrading from a version of SL1 prior to 11.1.0, you must first upgrade to an 11.x version of SL1 before you can upgrade to later versions.
- During the upgrade to 11.x, the user interface will be unavailable for several minutes.
- Versions of Global Manager prior to 11.1.0 will not work with SL1 11.1.0 or later.
- Web Proxy Services will not work in SL1 11.1.0 or later.
- PowerPacks built in SL1 version 11.1.0 and later releases cannot be imported into previous versions of SL1. However, PowerPacks built in releases prior to 11.1.0 can be imported into 11.1.0 and later.
- If you have created custom content in PHP, see this page for notes on backward compatibility: https://www.php.net/manual/en/migration70.incompatible.php

For more information on upgrading from 10.2.x or earlier, see the section on ***the 10.x to 12.2.0 upgrade path***.

Upgrading from Version 8.14.x or Earlier

NOTE: This section applies to users who are upgrading from SL1 8.14.x or earlier. If you are upgrading from SL1 10.1.0 or later, you can ignore this section.

SL1 version 10.1.0 included an upgrade from MariaDB 10.1 to MariaDB 10.4. Because of this upgrade, if you are currently running SL1 8.14.x or earlier, you ***must*** first upgrade to a 10.x release and the version of MariaDB that corresponds to that release, and then upgrade to an 11.x release and its corresponding version, before upgrading to later releases.

For more information on upgrading from 8.14.x or earlier, see the section on ***the 8.x to 12.2.0 upgrade path***.

In addition, if you are upgrading from 8.1.4.x or earlier, you should also be aware of the following updates before deploying 12.2.0:

- As of version 10.1.0, SL1 no longer includes Flash.
- As of SL1 8.12.2, ScienceLogic no longer updates the help that appears when you click the **[Guide]** button that appears in the classic user interface. Instead, you can click the **[Help]** button at the top of each page. Doing so opens a Help topic about that page. From that topic, you can then click a link to view additional information in the product documentation at ***docs.sciencelogic.com*** in a new browser window.
- As of SL1 8.10.0, SL1 does not support Data Collectors and Message Collectors running the CentOS operating system. If your system includes Data Collectors and Message Collectors running the CentOS operating system, contact your Customer Success Manager for details on upgrading Data Collectors and Message Collectors to Oracle Linux before installing the latest SL1 version.
- To download updates for previous SL1 versions that have reached their End-of-Life date and are no longer supported by ScienceLogic, contact ScienceLogic Support or a designated Customer Success Manager to get the update files.

Known Issues for SL1 Hollywood 12.2.0

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 12.2.0:

- The option to enable a Military Unique Deployment (MUD) configuration is not available for SL1 12.2.0 installations or upgrades. (Jira ID: EM-57752)
- 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)

- 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 IDs: EM-59433, EM-62316)

- After upgrading SL1 and MariaDB, all appliances should be on MariaDB 10.4.31. However, if your SL1 system is deployed on AWS and you go to the **Appliance Manager** page (System > Settings > Appliances) in SL1, the ***MariaDB*** field for your appliances might be highlighted and display a message that your appliances should be on 10.4.29. This highlighting and messaging can be ignored. (Jira ID: EM-59172)

- Some SL1 collectors that have been upgraded to 12.2.0 have experienced filesystems at or near 100%. (Jira ID: EM-62372)

- Some upgraded 12.2.0 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: (Jira ID: SLUI-18754)

  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.

- 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 12.2.0, 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)

- 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 most 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, EM-51165, EM-62364)

- After upgrading to 12.2.0, 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 **Event Insights** page is not loading properly in AWS Extended Architecture deployments. Additionally, the page is displaying incorrect "No Event Created" metrics for the following deployment types: AWS GovCloud, AWS Extended Architecture, on-premises Distributed Architecture MUD patches, and on-premises Extended Architecture systems. (Jira IDs: EM-58561, EM-59467)

- 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-17890)
  - Services that are added or created to the N-tier hierarchy have their ***RCA Options*** field set to *Disabled* by default. To work around this issue, you can manually set the field to *RCA Enabled (contributors only)*. (Jira ID: SLUI-18852)
  - 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 12.2.0, 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)
- "VMware: vSphere Base Pack" PowerPack v306 and v307 are not compatible with SL1 12.2.0, 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)
- After upgrading to SL1 12.2.0, you might receive an "Internal Server Error" in one of the following scenarios:
  - Immediately after using single sign-on (SSO) to log in to the default SL1 user interface (AP2)
  - Trying to log out from the default user interface while using SSO
  - Intermittently while using the default user interface, regardless of your authentication type

  Drop files are available to work around this issue. For more information, including workaround steps, see https://support.sciencelogic.com/s/article/13702.

- If you repeatedly sign in and out of SL1 in a short period of time, you might experience a spinning "loading" circle that prevents you from logging in again, or you might receive an error that temporarily prevents you from signing back in due to a caching issue. If this occurs, you can try one of the following workarounds: (Jira IDs: SLUI-15357, EM-62254)

    - Wait 5 minutes before attempting to sign in again.

    - Set caching for SL1 sessions to 0. Doing so avoids the issue by effectively turning off session caching, but this might result in performance issues or issues with Global Manager. To do so:

        1. Start an SSH session into your SL1 appliance.
        2. Using vi or another text editor, edit the `/opt/em7/nextui/nextui.conf` file. To do so, enter the following at the shell prompt:

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

        3. Add the following line at the bottom of the NextUI configuration file:

            ```
            AUTH_CACHE=0
            ```

        4. Save your changes (`:wq`) and then restart the NextUI service by running the following command:

            ```
            sudo systemctl restart nextui
            ```

    - Sign in using the classic SL1 user interface.

    For additional details about this issue, see https://support.sciencelogic.com/s/article/9715 or https://support.sciencelogic.com/s/article/13701.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

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.

ScienceLogic

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

International: +1-703-354-1010