ScienceLogic

SL1 Golden Gate 12.1.0 Release Notes

SL1 version 12.1.0 (Document revision 3)

SL1 Golden Gate 12.1.0 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 12.1.0.

The SL1 Golden Gate 12.1.0 release includes a number of key new features and enhancements:

- *Oracle Linux 8 support for new SL1 deployments*
- *CyberArk Vault support for credentials*
- *Global Manager support for Business Services*
- *Updates to the Event Insights page*
- *New Device Investigator layout and widget customization options*, plus the ability to bulk delete devices from the **Devices** page
- *A new Root Cause Timeline dashboard widget that integrates with Zebrium*, plus additional new dashboard widget customization options
- *A new default user account for the SL1 agent*
- Plus *many additional exciting updates*

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 Golden Gate 12.1.0

This section describes the features and enhancements that are included in SL1 Golden Gate 12.1.0.

Agent

- **What's new: *A new default user account*.** The Windows, Solaris, and AIX agent installation processes were updated to create a new dedicated "scilog" user account that runs the agent as a non-root/non-administrator user by default. The installation instructions on the Download/Install Agent dialog were updated accordingly.
- **For more information:** See *Installing the SL1 Agent*.

> IMPORTANT: In previous versions of SL1, the SL1 agent installed and ran as "root." With this update, the agent will install and run as the "scilog" user by default. However, you still have the option to continue running the agent as root if you choose.
>
> Your existing agents will continue to work in this version, but if you opt to use the new, default "scilog" user, you will need to update your current processes, automations, and internal documentation to account for the new "scilog" user.

> **NOTE:** The following agent versions are required for SL1 12.1.0:
>
> - Windows: 145
> - Linux: 184
> - AIX: 184
> - Solaris: 184

Additional Agent Updates

- Updated the Windows and Linux agents so that you can edit, add, or delete fields in the scilog.conf or scilog_proxy.conf files.
- Updated the error reporting interval to declutter the Windows Event log of known error events. Frequent errors will be repeatedly reported, but at a greater interval between reports than before.
- Orphaned agent records will no longer be created whenever agent registration fails due to device record linking errors.
- You can now run a streamer test directly from the Windows command line.
- Events will no longer be generated when the agent process still detects a Dynamic Application that has been unaligned in the user interface.
- Added an option to turn off agent log indexing services. This prevents empty messages from causing the log summarizers to crash.

- Re-enabled the GraphQL endpoint on the responder for agent-related queries. Firewall rules restricting access to the internal API endpoints are required.
- For custom and supported PowerShell Dynamic Applications, errors will now be written to the agent device logs. An internal alert will be cleared for PowerShell issues when they are resolved.
- Improved Processor Summary calculations by using the CPU Busy Percentage value that the agent sends instead of the CPU's time.
- Updated agent-monitored device alerts to occur only with latency of 1. Agent-monitored devices with an availability protocol of 5 will not trigger an alert.
- Updated the agent vitals process service to store process-related data and trigger related alerts every time agent data is uploaded to SL1. This upload will occur every five minutes by default.
- Optimized the process summary writer services so that process data continues to update when the legacy Scylla-backed agent pipeline is in use.
- Agent device logs were updated to write errors for tracking purposes even in scenarios where Dynamic Applications are not aligned to a device.
- Updated the PowerShell internal alerts service so that the outage created during a PowerShell issue is cleared when the issue is resolved. Subsequent alerts will not be raised again if the service is restarted.

Anomaly Detection

- **What's new:** ***The Anomaly Index chart.*** A new **Anomaly Index** chart was added to the **Machine Learning** page, the **[Machine Learning]** tab of the **Device Investigator**, and the **[Anomalies]** tab of the **Service Investigator**. This chart indicates how far the collected data for the metric diverges from its normal patterns. It displays values ranging from 0 to 100 and is color-coded by the level of event that gets triggered the further the data diverges.

  The following additional updates were made to support this new feature:

  - You can define the thresholds for the Anomaly Index, and whether those values generate alerts, on the **Machine Learning Thresholds** page (Machine Learning > Thresholds).
  - You can click an expand icon next to each device on the **Machine Learning** page to view the **Anomaly Chart** modal for that device.
  - When you hover over a value in one of the charts on the **Anomaly Chart** modal, a pop-up box appears that includes the Anomaly Index value and whether that value is normal, low, medium, high, or very high.
  - When the real metric data is missing, a pop-up message displays on the **Anomaly Chart** modal stating: "Actual values can't be retrieved. Only expected range can be displayed."
- **For more information:** See *Enabling Machine Learning-based Anomaly Detection*.

Additional Anomaly Detection Updates

- Added an ***Anomaly Count*** column to the **Machine Learning** page and the **[Machine Learning]** tab of the **Device Investigator** that lists the number of anomalies present on that device.
- Updated the Anomaly Detection status to display "Failed (building)" when no winners can be found for a predictor. SL1 will continue to monitor for anomalies on that device.
- The "SL1: Anomaly Index Event Monitoring" PowerPack was updated to use API alerts instead of internal alerts.

Credentials

- **What's new: *CyberArk Integration*.** A credential gateway service was introduced that allows you to download the CyberArk agent from your own instance of CyberArk and install the CyberArk agent on SL1 Data Collectors. When an SL1 system has been set up with the CyberArk agent and the credential gateway service, you can enter vault tags in any secret/encrypted credential field in SL1 instead of entering the password or secret value itself. The agent syncs with credentials on the CyberArk Vault server and uses those credentials to collect data from SL1 monitored devices when necessary.
- **For more information:** See *Using External Credential Services*.

> **NOTE:** CyberArk is not provided with SL1. You must purchase and manage the CyberArk Vault independently.

Additional Credentials Updates

- Added a new credential type, "SL Service Connection". This credential type is automatically created when a new *service connection* is created.

Dashboards

- **What's new: *A Root Cause Timeline widget that integrates with Zebrium*.** A new Root Cause Timeline widget type was added for AI/ML Predictions. This widget type lets you see when the Zebrium AI/ML (machine learning) engine detects a possible or confirmed issue. When you hover over an icon for a suggestion or an alert in the widget, a pop-up displays a title and a word cloud that contains root cause information. You can click an icon in the widget to drill down into the Zebrium user interface to view a detailed Root Cause report.
- **For more information:** See *Creating and Editing Dashboards*.

Additional Dashboards Updates

- Added a dashboard list widget type that displays the list of dashboards that appear on the **Dashboards** inventory page.
- Made the following updates to event table widget types:
  - Added a ***Masked Events*** properties column.
  - Added the ability to add or edit notes to specific events by clicking the icon under the ***Event Note*** column.
  - Added **[Acknowledge]** and **[Clear]** buttons.
- Updated device component table widget types to display the parent for each device. You can click the parent device name to go to the **Device Investigator** for that parent device.
- You can now change widget title names when in edit mode.
- You can now edit column filter settings for table/leaderboard widget types.
- Dialog messages no longer display when you favorite or unfavorite dashboards unless the actions are unsuccessful.

Deployment

- **What's new:** ***Oracle Linux 8 support for new SL1 installations.*** A new Oracle Linux 8 (OL8)-compatible installation wizard was added to the SL1 ISO file. All new SL1 12.1.0 installations will include OL8 by default.
- **For more information:** See *Installation and Initial Configuration*.

> **NOTE:** Users who are upgrading to SL1 12.1.0 from an earlier release are unable to convert to OL8 with this release. Those upgraded SL1 systems will continue to use OL7. The ability to convert to OL8 from an existing OL7 SL1 instance is planned for a release in the near future.

> **NOTE:** The option to enable a Military Unique Deployment (MUD) configuration is not available for SL1 12.1.0 installations or upgrades.

Additional Deployment Updates

- The process for installing SL1 on Azure using VHD image files has been simplified. For more information, see the *Installation and Initial Configuration* manual.
- Data Collector and Message Collector images are available from the Azure Marketplace. This allows customers who deploy SL1 in Azure environments to add Data Collectors and Message Collectors without the need to request and wait for an image.

- Added the ability to use two new configurable fields in the silo.conf file. These fields, ap_user and ap_pass, enable you to define usernames and passwords for the Administration Portal that differ from the usernames and passwords used for the Database Server.

Devices

- **What's new:** ***New Device Investigator layout and customization options.*** The default layout for the **Device Investigator** has been redesigned for enhanced readability and to provide a quicker assessment of the device state and contextual data. Additional updates to the **Device Investigator** include:
    - New customization options, including the ability to customize widget widths.
    - Visual updates to the **Events** and **Logs** widgets.
    - The ability to view interface network utilization graphs in a new window by clicking the bar graph icon next to the interface name from the **[Interfaces]** tab.
- **For more information:** See *Using the Device Investigator*.

Additional Devices Updates

- You can now bulk-delete devices from the **Devices** page.
- Added a footer to the **Devices** page that displays the total number of devices selected and the total number of rows on the page.
- Dialog messages no longer display when you favorite or unfavorite devices unless the actions are unsuccessful.

Events

- **What's new:** ***Updates to Event Insights.*** The following updates were made to the **Event Insights** page:
    - Added a new "Savings" section that highlights a system's "noise reduction" percentage and the estimated time saved from SL1's noise reduction and deduplication capabilities compared to the estimated amount of time it would take to triage an SL1 event. This section includes all event severity levels when calculating savings.
    - Added a new "Tuning Targets" section that displays the top 10 most utilized event policies and top 10 noisiest devices by event volume during a selected time frame. You can also download CSV reports of this data.
    - Renamed the "Overview" section to "Event Trends" and added two new charts. These charts display:
        - The ratio of total events created to the number of active devices during a selected time frame
        - The ratio of masked events to the total events created during a selected time frame
    - Added the ability to download all of the Event Insights Sankey chart data into a CSV report.

    - Added new mouse-over features to the Sankey chart that allow you to:
        - View the total count of records that did not result in an event being created and the various reasons as to why an alert did not generate or update an event record.
        - View alert node values related to your system's event links and review any alert source context related to new event record severities.
        - View counts for each severity category in the "New Event Created" and "Deduplication" nodes.
        - View API alert node values related to your system's nodes. The metrics include a total count of alerts represented by that node and a breakdown of the three event classifications: "New Event Record," "Deduplication," and "No Event Created." Metrics depicted are based on the time span selected by the page's time selector feature.
- For more information: See *Event Insights*.

Additional Events Updates

- On the **Events** page, you can now filter active event records in the ***Event Note*** field.
- Updated the **Event Details** page to the hide the **Assets** and **Vitals** panels if there is no data present.
- If you click an event relating to a specific device on the **Event Investigator**, you will now be redirected to the **Device Investigator** for that device. An event context panel will appear at the top of the page, where you can clear, acknowledge, or view causes and resolutions relating to the event.
- Updated the color and styling of the event severity chips.

> **NOTE:** There is a *known issue* that impacts this enhancement.

Global Manager

- **What's new:** ***Business Services support***. Global Manager now includes support for Business Services. This enhancement enables you to aggregate business service views across multiple SL1 stacks. The following changes were made to support this enhancement:
    - Added the Business Services icon to the side navigation bar for Global Manager systems.
    - Global View mode is permanently toggled on (blue) for business services in Global Manager systems. It cannot be toggled off.
    - Added the ***Stack ID*** column to the **Business Services Inventory** page in Global Manager systems to identify which business service belongs to which stack.
    - Added Global Manager support to the Change Events widget and the **[Services]** tab.
    - Updated the Sunburst and Relations List component to now support business services in Global Manager systems.
- **For more information**: See *Viewing Global Business Services*.

Additional New Features and Enhancements in SL1 Golden Gate 12.1.0

Access Control

- Added four new access hooks: DYN_APP_ADD, DYN_APP_EDIT, DYN_APP_REMOVE, and DYN_APP_VIEW. Respectively, these access hooks enable you to add, edit, delete, and view Dynamic Applications using the SL1 user interface or GraphQL.
- Updated the descriptions for the SYS_DYN_APP_ADDREM, SYS_DYN_APP_EDIT, and SYS_DYN_APP_MANAGEMENT access hooks to specify that they are applicable only to the classic SL1 user interface and REST API.

Authentication

- Added a new ***User Login Session Timeout*** setting on the **Behavior Settings** page (System > Settings > Behavior) that lets you define the amount of idle time that can pass without any user activity before that user's SL1 session expires. By default, user sessions expire after 10 minutes of inactivity.
- Updated the default maximum number of simultaneous user sessions to 300.

Business Services

- If you click an event relating to a specific device on the **Service Investigator**, you will now be redirected to the **Device Investigator** for that device. An event context panel will appear at the top of the page, where you can clear, acknowledge, or view causes and resolutions relating to the event.
- Dialog messages no longer display when you favorite or unfavorite services unless the actions are unsuccessful.

Collector Pipeline

- Updated set_cpl.py to use Python 3 by default, but with backward capability to Python 2.

Custom Attributes

- Added a pruner to hourly maintenance to remove orphaned custom attributes from SL1.
- Implemented a new custom attribute dynamic rule operator to search by empty value.

Data Collection

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

> IMPORTANT: If you are upgrading to 12.1.0 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 the upgrade, you can go to the **Appliance Manager** page (System > Settings > Appliances) to determine which appliances might require a reboot.

- Added the ability to use Collector Unit Postprocessing Service (CUDAPS) by default instead of Dynamic Application collection for data postprocessing. To enable this feature, you must insert the field enable_cudaps_service_default with a value of "1" into the master.system_custom_config database table.
- Legacy PowerShell and WMI snippets are both Python 2- and Python 3- compatible and are provided through the sl_snippets library.
- The following collection types are now Python 2- and 3-compatible:
    - Critical availability collection
    - Interface collection
    - Port monitoring
    - Process inventory and performance collection
- Added Python 3 compatibility to pypsrp, pykerberos, pywinrm dependencies, and related libraries.
- Updated specifications for set_cpl.py so that an error occurs if you try to enable/disable 'Filesystem'.
- Updated specifications for da_conf so that it is not an option unless you specify 'da_conf' to be enabled/disabled.

Data Retention

- Updated the pruning queries for "EM7 Core: Hourly Maintenance" and "EM7 Core: Daily Maintenance" for optimization and speed.

Device Groups

- Updated Device Group queries, including Device Group-related queries for IT services, for optimization and speed.

Documentation

- The following enhancements were made to the ***Product Documentation site***:
    - The home page and left-hand navigation were streamlined to focus on the core ScienceLogic products: SL1, PowerFlow, PowerPacks, and PowerFlow SyncPacks, plus docs for SL1 Developers, Restorepoint, and Zebrium. The ***Release Notes site*** also now follows the same structure and uses the same icons.
    - A new link icon appears next to headings for topics and sub-topics. You can click the icon to share or save a link to that specific location in the documentation.
    - Code text now appears with a gray background and bigger margins for easier reading. Additionally, large chunks of code are now contained in expanding/contracting sections for less scrolling.
    - New Product Life Cycle pages were added for ***SL1*** and ***SL1 PowerFlow***.
- The ***Product Release Notes site*** was also updated to include release notes for the latest SL1, PowerFlow, PowerPack, SyncPack, Restorepoint, and Zebrium releases.

GraphQL

- Made the following GraphQL updates to support the management of host files:
    - Added a new GraphQL resource for "HostFileEntry" that allows you to query host file entries. You can search for host file entries by "id", "ipAddress", "hostnames", "organization", or "collectorGroup".
    - Added a new "createHostFileEntry" mutation that allows you to create a single host file entry. Entries created with this mutation will sync with all Data Collectors aligned to a given collector group and be written to the Data Collectors' host files ("/etc/hosts").
    - Added a new "updateHostFileEntry" mutation that allows you to edit existing host file entries.
    - Added a new "createHostFileEntries" mutation that allows you to create multiple host file entries. This mutation has one required argument: a headerless CSV file with one host file entry per line. Each line should have five comma-separated values: "IP address", "hostnames" (space-separated, valid hostnames, 255 characters maximum), "description", "organization ID", and "collector group ID".
    - Added three new bulk-delete mutations for host file entries: "deleteHostFileEntries", "deleteHostFileEntriesByCollectorGroup", and "deleteHostFileEntriesByOrganization". Respectively, these mutations allow you to bulk delete entries by "entry ID", "collector group ID", or "organization ID".

- Made the following updates to support Zebrium ***service connections***:
    - Created a required "deploymentId" field for Zebrium service connection configurations.
    - Added the "serviceConnection", "zebriumConnection", "serviceConnections", and "zebriumConnections" queries. These queries enable you to query for a specific connection by ID or all connections.

      NOTE: The "zebriumConnection" and "zebriumConnections" queries expose a "host" field, which is also available in the JSON returned in the "configuration" field.

    - Added the "createServiceConnection", "createZebriumConnection", "updateServiceConnection", and "updateZebriumConnection" mutations. These mutations let you create or update service connections that store a Zebrium access token and related configuration details for connecting to Zebrium APIs.
    - Added two new bulk delete mutations, "deleteServiceConnections" and "deleteZebriumConnection", to support deleting one or more existing service connections.
- Made the following updates to support Dynamic Application snippet configurations:
    - Added a new "DynamicApplicationSnippetConfiguration" GraphQL resource.
    - Added the "createSnippetConfigurationSnippet", "updateSnippetConfigurationSnippet", and "deleteSnippetConfigurationSnippet" mutations to create, update, or delete Dynamic Application snippet configurations, respectively.
- Added a new "deleteDevs" mutation that allows you to delete multiple devices at once in GraphQL.
- Added a new "toggleSetupConfigWorkflowsApplicability" mutation that allows you to "dismiss" a Setup and Config workflow if deemed not applicable.
- Added the ability to disable schema introspection in GraphQL. Introspection is still enabled by default, but you can now disable it in the nextui.env file.

  To do so, use SSH to access your SL1 appliance, log in as an administrator, open the nextui.env file (`sudo vi /opt/em7/nextui/nextui.env`), change the `GQL_INTROSPECTION` field to `GQL_INTROSPECTION=disabled`, and save the nextui.env file.

  Then, open the nextui.conf file (`sudo vi /opt/em7/nextui/nextui.conf`), add a new line at the bottom that says `GQL_INTROSPECTION=disabled`, and save the nextui.conf file.

  To re-enable introspection, follow the same instructions but in both files, change `GQL_INTROSPECTION` to `GQL_INTROSPECTION=enabled`.

High Availability and Disaster Recovery

- Updated coro_install to deploy a high availability cluster without requiring a cross-over cable between the nodes.
- Updated the setup wizard and supported methods for clustering classic Database Server appliances to support Oracle Linux 8 (OL8).

Licensing

- Restored the ability to license SL1 appliances using the classic Web Configuration Utility, which had been removed in SL1 11.2.0. The classic Web Configuration Utility can be accessed at <IP address>:7700.

Logging

- Updated event engine syslog message processing to support the upgrade to Oracle Linux 8 (OL8).

> **WARNING:** If you are upgrading to SL1 version 12.1.0 from a version prior to 11.3.0, then any existing modifications you made to your rsyslog configurations to support log forwarding, filtering, or TLS reception in previous versions will be removed. To reconfigure any custom rules using the appropriate syntax, see the "Logging in SL1 Version 11.3.0 and Later" topic in the ***Daily Health Tasks*** section of the ***System Administration*** manual.

- To support the upgrade to OL8, audispd configuration options are now part of auditd.conf. In addition, the plugins.d directory has been moved under /etc/audit. The current status of auditd and its plug-ins can now be checked by running the service auditd state command.

Organizations

- Increased the character limit from 64 to 128 for organization names.

Platform

- The use of iptables is removed along with all of the legacy rules files to support legacy iptables syntax in SL1 12.1.0. With this change, the following files are no longer referenced when defining firewall configurations:
  - /etc/sysconfig/iptables
  - /etc/sysconfig/ip6tables
  - /etc/siteconfig/iptables-phonehome
  - /opt/em7/share/config/iptables.d/*.conf

  As of SL1 12.1.0, custom firewall rules need to use rich rules syntax and must be added to /etc/siteconfig/firewalld-rich-rules.siteconfig.

> **IMPORTANT:** Users who are upgrading to SL1 12.1.0 from an earlier version must proactively convert their custom firewall rules to use rich rules syntax and add them to /etc/siteconfig/firewalld-rich-rules.siteconfig.

- SL1 12.1.0 includes the following updates:
  - Kubernetes 1.24+rke2r1
  - Docker Compose v2.17.2

PowerPacks

- The 12.1.0 ISO includes the following new or updated PowerPacks:
  - Microsoft: Azure v118
  - Supplemental Device Classes v103
- Updated the Compaq device class names to HPE in the "Supplemental Device Class" PowerPack.
- *Deprecated and removed multiple PowerPacks* from the 12.1.0 ISO.

ScienceLogic Support Pack

- The "ScienceLogic Support Pack" PowerPack was updated to ensure compatibility with Oracle Linux 8 (OL8).

Security

- 12.10 includes multiple package updates to improve security and system performance.

Service Connections

- Added a new **Service Connections** page (Manage > Service Connections) that enables you to view, edit, and delete existing service connections and create new ones. A service connection stores configuration details, including an API key or access token, which is used to connect SL1 to external data resources, such as the Zebrium API.

Setup and Config Page

- Added a **[Reset]** button to the **Setup and Config** workflow cards that allows you to reset one or more of your workflows.
- Added a new **[Not Applicable]** button to the "Not Started" workflows section under the ellipses drop-down. When you click this button, it sets the selected console workflow as "Not Applicable," which moves the workflow to the bottom of the page and out of the immediate page view. You can also display a previously set "Not Applicable" workflow by selecting that workflow and clicking **[Display]**.
- The **Setup and Config** workflow cards are now grouped together and displayed based on their workflow statuses. Each workflow section is collapsible and expandable. The workflow count is displayed in the status/section header. However, if a workflow count is zero, it appears grayed out.
- Updated the **Setup and Config** workflows to automatically update to a "Not Applicable" status when you select the "Not Applicable" option from the workflow status bar or when any activities within that workflow's cards are also marked as "Deactivated" or "Not Applicable".
- Updated the **Activity** wizard on the **Setup and Config** page to automatically update the activity status of a completed task to "In Progress."
- When you close the **Activity** wizard or complete a task, you now return automatically to the **Setup and Config** page with the activity's status updated to reflect your progress.

System Administration

- Implemented the Python 3 port for the patch manager service. With this change, siloupdate-manager.service replaces em7_patch_manager.service.

System Update

- Updated the system update process for Python 3 compatibility. Several changes were made to support this update:
    - The em7_patch_manager service that was responsible for managing patch operations was replaced with a new siloupdate-manager service. This systemd service manages all patch operations including deployment, which was previously managed as an asynchronous process.
    - Logs relating to deployment operations, which previously were written to /var/log/em7/patcher.log, are now written to /var/log/em7/patch_manager.log.
    - For staging and preupgrade, SL1 appliances are processed in batches according to the pool_size parameter, but deployment is triggered for all eligible appliances at once.
    - The `pcli import-patch` command is not supported in SL1 12.1.0. Support for this command will be restored in a future release.
    - The `pcli monitor_stage` and `pcli monitor-deploy` commands are not compatible with SL1 12.1.0.
- Added a new mode to the staging phase of the SL1 siloupdate service. This new "enhanced file upload" mode causes pre-staging operations and file upload operations to happen in separate processes so file upload time is not counted towards the staging wait time setting. This mode is on by default, and ScienceLogic recommends leaving it on due to the large amount of data that can be pushed during SL1 upgrades.

  However, it is possible to turn this setting off or to change other settings relating to enhanced file upload mode by adding or updating entries in the "master.system_settings_patcher" database table:

    - To turn off the setting, insert the parameter "use_enhanced_file_upload" and the value "0".
    - To change the number of file upload workers, insert the parameter "num_file_upload_workers" and set the value to your preferred number of workers. The default value is 12.
    - To change the number of pre-staging workers, insert the parameter "pool_size" and set the value to your preferred number of workers. The default value is 25.
- Updated the System Status script, system_status.sh, for SL1 12.1.0. These updates included added support for remote databases and Oracle Linux 8; updated logic and checks for DRBD, Corosync, and Pacemaker; updated logfile locations; and additional fixes.

User Interface

- The basic menu and the Advanced menu were updated to display links for only the pages to which you have access.

- The [Anomalies] tab on the **Service Investigator** was 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.
- Updated the **Add Node** wizard (Manage > Nodes > Add Node) to display as a standalone page instead of as a modal overlaid on top of the **Nodes** page.

Zebrium Integration

- You can now create a ScienceLogic Widget Integration in the Zebrium user interface. You can use the values for the Endpoint, Deployment ID, and Access Token in that integration to create the SL1 *Root Cause Timeline* widget to monitor suggestions and alerts for Zebrium in SL1.

> **NOTE:** The Deployment ID can be found on the new **Service Connections** page (Manage > Service Connections) in SL1.

Issues Addressed in SL1 Golden Gate 12.1.0

This section describes the issues that were addressed in SL1 Golden Gate 12.1.0.

Agent

- Resolved an issue in which the Windows agent failed to upload a data file, causing a "Device Failed Availability Check: ICMP Ping" event. (Cases: 00316258, 00322719, 00324387)

Asset Management

- Updated the ***Installed Memory*** field on the **Asset Configuration** page (Registry > Assets > Asset Manager > wrench icon > Configuration) to operate as expected. (Case: 00224344)

Authentication

- Addressed an issue that was allowing users to remain logged in even after their user sessions were terminated from the **Access Logs** page (System > Monitor > Access Logs). With this update, all users will be forced to log back in to SL1 if their session is terminated from that page. (Case: 0021241) (Support ID: 175960)

Classic IT Services

- To address unhandled exceptions in classic IT services, the PHP formula processor was updated to return a properly encoded JSON string. The update now prevents the PHP formula processor from returning an empty string. (Cases: 00235152, 00264093)

Credentials

- Updated SOAP/XML credentials to ensure that the port in a URL string that includes a % symbol is stored as the user-specified port value. (Case: 00284539)
- Updated the SNMP Read/Write credential template to ensure deleted credentials are removed. (Case: 00189403)

Custom Attributes

- Addressed an issue where a Dynamic Application could not update a custom attribute if the custom attribute was updated or deleted. (Case: 00167804)

Dashboards

- Addressed an issue where users were unable to create dashboard schedules in the SL1 user interface. (Case: 00179733)
- Updated dashboard widgets to display and represent null data by the presence of axes. Additionally, removed the "No Data" message that appears on widgets that display null data. (Case: 00228205)
- Addressed an issue in which scheduled dashboards in the classic SL1 user interface failed to export and email the dashboard to users. (Case: 00251107)
- Updated the dashboard image that is sent to recipients when scheduled dashboards are generated in the classic SL1 user interface to ensure that the entire image can be viewed. (Case: 00133754)
- Updated the **Devices** widget on the **Dashboards** page to save filters that contain component object-related searches. (Cases: 00229813, 00318595)

Data Collection

- Addressed an issue where the powershell_collector.env MAX_KINIT_TIMEOUT was treating any setting greater than 30 seconds as 10 seconds. The powershell_collector.env now allows MAX_KINIT_TIMEOUT to be a maximum of 60 seconds. (Case: 00271487)
- Addressed an issue where erroneous custom attributes were created from Database Configuration Dynamic Applications. (Cases: 00147516, 00202046)
- Addressed an issue that was causing the "Data Collection: Interface Bandwidth" process to generate unhandled exceptions when devices were polled for Interface Bandwidth. (Case: 00278779)
- Addressed an issue in which SNMP collections were missed by the Concurrent SNMP Collection Service during unexpected service restart. (Case: 00288208)
- Updated several data pull Dynamic Applications to ensure that they properly report collector IP addresses. (Case: 00280678)

Data Retention

- Updated a pruner process for master.topo_comp_relationship to remove orphaned relationships from a deleted device. (Case: 00266629)

Device Groups

- Updated device group queries for optimization and speed. (Cases: 00269018, 00270135, 00270608, 00273876)

Device Templates

- Updated device templates to ensure the device's disabled ***Collection Objects*** column displays proper data and stops collection. (Case: 00199692)

Devices

- Improved the page load time for the **Device Dashboards** page (System > Customize > Device Dashboards) in the classic SL1 user interface. (Cases: 00261967, 00279846)
- Updated device categories to remove Dynamic Component Mapping restrictions. (Cases: 00055069, 00073688, 00095820, 00098262, 00244536)
- Updated the **Interfaces** page (Devices > Device Manager > Wrench > Interfaces) to display all of your device interfaces given you have the proper "View" permissions set to your account. (Case: 00306690)
- When a device is deleted by the "EM7 Core: Hourly Maintenance" process, any component mappings related to that device will be removed. This ensures that no issues occur if a physical device is unmerged whose component counterpart has been deleted. (Case: 00264907)
- Updated the "network.router" category to allow you to create child devices. Even if you switch this category to another, and then switch back, the existing child devices will remain. (Cases: 00215936, 00252697)
- Updated the device deletion process to ensure that device and device group event suppressions are removed completely. (Case: 00260994)

Discovery

- Updated IP address lengths to pass correctly during the discovery process. (Cases: 00292275, 00298389, 00300580, 00307556, 00309404, 00310906, 00314828, 00322907, 00324427, 00330133)

Documentation

- Updated the *High Availability and Disaster Recovery Configuration* manual with a new chapter detailing the process to ensure DRBD is in sync between nodes during DR and HA failover. (Case: 00201292)
- Updated the *Dashboards* manual to clarify that using the time span filter does not impact the list of events that appears in Events table widgets. (Case: 00356619)
- In the *System Administration* manual, overhauled the section on *Backup Management* and updated the instructions for *changing the MariaDB password*. (Case: 00337108)
- Updated the *Customizing the SL1 User Experience* manual to correct some definitions for fields that can be included in tabbed forms. (Case: 00363085)
- Added a note in the *Introduction to SL1* manual cautioning users against using multiple "ANY" options for

multiple search terms when performing a basic search, as doing so can cause issues with search query performance. (Case: 00363447)

Dynamic Applications

- Updated the **Dynamic Application Manager** page (System > Manage > Dynamic Apps) to ensure the ***Last Edited*** and ***Edited By*** column values are updated properly when a bulk update is performed. (Case: 00302291)
- Increased the number of records that journal Dynamic Application storage tables can store. (Case: 00280951)

Events

- Updated the ***Last Edited*** field on the **Event Policy Manger** page (Registry > Events > Event Manager) in the classic SL1 user interface to reflect any updates made in the **[Suppressions]** tab of the **Event Policy Editor**. (Cases: 00231086, 00252998)
- Updated the **Tools** widget in the **Event Investigator** to display "Default Tools" for a device-based event. (Case: 00250193)
- Updated the event engine and automation engine to retrieve and evaluate device relationships in a predetermined order when selecting the first parent-child relationship between devices. Relationship types now process in this order:
  1. Ad hoc/Manual
  2. Layer3, LLDP
  3. CDP, Layer2
  4. VM

  (Cases: 00216002, 00252998)
- Updated the event engine to stop generating exceptions for "trap" event types when the ***Identifier Format*** field includes a special character. (Case: 00226646)
- Updated the ***Last Detected*** column on the Events page to sort by date rather than alphabetical order. (Case: 00345546)
- Updated the Events page to ensure the page scrolls as intended when viewing the list of events grouped by organization. (Cases: 00303177, 00307521, 00312281, 00341701)

High Availability and Disaster Recovery

- Addressed an issue that was causing the "EM7: DRBD Failover Primary" event policy to falsely trigger an alert when the relevant collection objects registered as "0" (zero) for a polling cycle due to a missed collection or failover. With this update, the DRBD Failover Primary alert formula now checks if the prior value is non-zero to ensure that it does not alert if no data exists. (Cases: 00125462, 00128562, 00130154, 00132711, 00144544)

PhoneHome Collection

- Added a new command line interface command to rename an existing PhoneHome device: `phonehome rename <new name>`. Previously, this was available using the `phonehome set <id>` command. (Case: 00293367)

PowerPacks

- Addressed an issue where a duplicate record in the filestore selected old metadata while installing a PowerPack, causing the installation to fail. (Case: 00273248)

Run Book Actions and Automations

- Addressed an issue that was causing Run Book Action snippets that used the "requests" library to not run successfully. This would result in the message "Unknown database 'master_access'" appearing in the device log. (Case: 00347084)

Schedules

- Updated the maintenance schedules that use the Asia/Kolkata time zone to correctly run from start to finish. (Case: 00322562)

ScienceLogic Support Pack

- Updated the "Support: Appliance Validation" Dynamic Application in the "ScienceLogic Support Pack" PowerPack to address an issue where null values were present when the Dynamic Application checked appliance sizing. (Case: 00220876)
- Updated the "Support: VMware Performance" Dynamic Application in the "ScienceLogic Support Pack" PowerPack to address an issue that was causing an OID error for NUMA collection objects on non-NUMA systems. (Case: 00326010)

System Update

- Updated the SL1 upgrade process to prevent legacy storage objects from causing unhandled exceptions. (Cases: 00182227, 00219887)

User Accounts

- Resolved an issue in which non-administrator users were unable to access all organizations and devices due to a "GraphQL Error: Forbidden" error. (Case: 00301056)

User Interface

- Updated the **[Registered]** tab of the **Nodes** page (Manage > Nodes) to increase the number of appliances that display to 25 and to automatically display the next 25 appliances when you scroll to the bottom of the list. (Cases: 00319543, 00320829)

- Ensured that only administrators can see the following pages in the classic SL1 user interface:
  - **Administer Bookmarks** page (Misc > Bookmarks)
  - **Regular Expression Tester** page (Misc > Regular Expression Tester)
  - **SL1 License Info** page (Misc > SL1 License Info)

  (Case: 00253683)

Recently Deprecated Features

12.1.0

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

> **NOTE:** If you are upgrading from a previous version of SL1, the 12.1.0 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 12.1.0 ISO due to a ***known issue***. It is still available for SL1 systems that upgrade to 12.1.0 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.

11.1.0

- Removed Flash-based pages in Views > Other Views.
- The Flash-based System Usage Pie Chart has been deprecated and is no longer available on the system usage report.

- Removed Flash-based Hardware Inventory graph.
- Removed Flash-based Maps.
- Removed the Flash-based Org Clock.
- Removed the Flash-based Map Icon column in the Device Category Register.
- Removed the Flash-based Ticket Timeline report.
- Removed the Flash-based Event Overview report.
- The 11.1.0 release deprecated the following PowerPacks and removed them from the ISO:
    - Cisco: CUCM Dashboards
    - Cisco: Old Cisco Apps
    - Cisco Unity Pack
    - LayerX Cisco CDR
    - Link Layer Neighbor Discovery
    - Microsoft: Azure Classic
    - Microsoft: Exchange Server 2010
    - Microsoft: Exchange Server 2010 Dashboards
    - Microsoft: Lync Server 2010
    - Microsoft: Lync Server 2010 Dashboards
    - Microsoft: Windows Server Services. Its content now resides in the Microsoft Windows Server PowerPack v112 or later.

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 Golden Gate 12.1.0

This section includes important notes for upgrading existing SL1 systems to the Golden Gate 12.1.0 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 12.1.0.

Supported Upgrade Paths

The SL1 10.1.0 and 11.1.0 releases both included major updates that you must consume before you can upgrade to 12.1.0. 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 12.1.0.

You can upgrade to SL1 12.1.0 using one of the following upgrade paths:

- *11.x to 12.1.0*
- *10.x to 11.x to 12.1.0*
- *8.x to 10.x to 11.x to 12.1.0*

See the sections below for additional details.

Upgrade Path 1: 11.x to 12.1.0

If you are currently running one of the following 11.x versions of SL1, you can upgrade directly to 12.1.0:

- 11.3.0 to 11.3.1
- 11.2.0 to 11.2.3
- 11.1.0 to 11.1.6

After upgrading to SL1 12.1.0, you must also upgrade to MariaDB 10.4.29.

Upgrade Path 2: 10.x to 12.1.0

In SL1 11.1.0, all PHP code was converted to PHP 7. Because of this change as well as changes made to the siloupdate-manager service in 12.1.0, if you are currently running a 10.x version of SL1, you ***must*** first upgrade to an 11.x version and the version of MariaDB that corresponds to that release before you can upgrade to 12.1.0 and MariaDB 10.4.29.

Therefore, if you are currently running version 10.x, then the upgrade to SL1 version 12.1.0 might require up to four (4) maintenance windows:

1. Upgrade to SL1 version 11.x.
2. Upgrade to the *MariaDB version that corresponds to that SL1 release*.
3. Upgrade to SL1 version 12.1.0.
4. Upgrade to MariaDB 10.4.29.

For detailed instructions on planning an upgrade, best practices for upgrades, and executing an upgrade, see the section on *Upgrading SL1* in the *System Administration* manual.

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 3: 8.x to 12.1.0

If you are currently running a version of SL1 8.x, you ***must*** first upgrade to the following releases prior to upgrading to 12.1.0, 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.

Therefore, if you are currently running version 8.14.x or earlier, then the upgrade to SL1 version 12.1.0 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. Upgrade to SL1 version 12.1.0.
8. Upgrade to MariaDB 10.4.29.

For detailed instructions on planning an upgrade, best practices for upgrades, and executing an upgrade, see the chapter on "Upgrading SL1" in the ***System Administration*** manual or view that chapter *online*.

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*.

Oracle Linux 8 Conversion

In SL1 12.1.0, all new SL1 installations include Oracle Linux 8 (OL8) as the default operating system.

However, users who are upgrading to SL1 12.1.0 from an earlier release are unable to convert to OL8 with this release. Upgraded SL1 systems will continue to use OL7 in 12.1.0. The ability to convert to OL8 from an existing OL7 SL1 instance is planned for a release in the near future.

NOTE: New SL1 installations that include OL8 have a required MariaDB version of 10.4.28. Upgraded systems that are still using OL7 have a required MariaDB version of 10.4.29.

Rebooting SL1 and Upgrading MariaDB

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

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

SL1 Release	Requires Appliance Reboot?	Required MariaDB Version
12.1.0 Upgrade (OL7)	Yes	10.4.29
12.1.0 ISO (OL8)	N/A	10.4.28
11.3.1	Yes	10.4.28
11.3.0	Yes	10.4.26
11.2.3	Yes	10.4.28
11.2.2	Yes	10.4.26
11.2.0	Yes	10.4.24
11.1.6	Yes	10.4.28
11.1.5	Yes	10.4.26
11.1.4	Yes	10.4.26
11.1.3	Yes	10.4.25
11.1.2	Yes	10.4.24
11.1.1	Yes	10.4.22

SL1 Release	Requires Appliance Reboot?	Required MariaDB Version
11.1.0	Yes	10.4.20
10.2.7	Yes	10.4.27
10.2.6.1	Yes	10.4.26
10.2.6	Yes	10.4.26
10.2.5	Yes	10.4.22
10.2.4.1	Yes	10.4.22
10.2.4	Yes	10.4.22
10.2.3	Yes	10.4.21
10.2.2	Yes	10.4.18
10.2.1	Yes	10.4.18
10.2.0	Yes	10.4.18
10.1.8.1	Yes	10.4.21
10.1.8	No	10.4.21
10.1.7	No	10.4.18
10.1.6	Yes	10.4.18
10.1.5	Yes	10.4.12
10.1.4	Yes	10.4.12
10.1.3	Yes	10.4.12
10.1.2	No	10.4.12
10.1.1	Yes	10.4.12
10.1.0	Yes	10.4.12

NOTE: For instructions on rebooting the SL1 system or updating MariaDB, 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.

SSH Collector Removal

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.

If you are upgrading to 12.1.0 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.

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 12.1.0, 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. At that time, any custom Python code that you have written within SL1 will cease to work properly. Therefore, if you currently use custom Python 2 code, ScienceLogic strongly recommends that you proactively convert it to use Python 3 instead.

Additional information about this change will be in the release notes and related documentation for the SL1 version in which Python 2 support is deprecated.

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.

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 12.1.0:

- 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 12.1.0 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 12.1.0:

- 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 12.1.0:

- 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 12.1.0. 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 12.1.0:

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 12.1.0 until all pre-upgrade tests are successful on all PhoneHome Database Servers.

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 12.1.0.
- During the upgrade to 12.1.0, 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

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 you can upgrade to SL1 12.1.0.

For more information on upgrading from 8.14.x or earlier, see the section on *the 8.x to 12.1.0 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 12.1.0:

- 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 Golden Gate 12.1.0

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 Golden Gate 12.1.0:

- The option to enable a Military Unique Deployment (MUD) configuration is not available for SL1 12.1.0 installations or upgrades.
- 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 known issue that is causing a lag in the deployment status reaching the Database Server after the default timeout value of 3600 seconds (1 hour). To 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.
- After installing or upgrading to SL1 12.1.0, 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.
- 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.
- When deploying SL1 on AWS using the 12.1.0 AMI, you must take additional manual steps to set up the "clientdbuser" password in MariaDB. This requires you to edit the /etc/silo.conf file. If you do not, you will not be able to access the user interface and a banner message about the database password not being set will appear after you log in to the appliance using SSH. For additional details about this issue, see: https://support.sciencelogic.com/s/article/9875.

- CPU, memory, and swap vitals metrics might not appear in the default user interface ("AP2") for newly discovered devices for several hours due to a known issue with data normalization. This issue does not impact previously discovered devices or devices in the classic SL1 user interface, nor does it cause any data loss. To work around this issue, log in to the console of the Database Server as an administrator and run the data normalization process in debug mode using the following command:

  ```
  sudo -u -s-em7-core SILO_DEBUG=1 /opt/em7/backend/data_normalizer_
  d.py
  ```

- A known issue might cause high swap usage in excess of 95% to be observed on appliance types running SL1 12.1.0 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.

- There is a known issue impacting users who upgrade from SL1 11.3.x to 12.1.0 that might cause events of only one severity type to appear on the **Events** page. When a user filters on a specific event severity in 11.3.x and then upgrades to 12.1.0, SL1 maintains that event severity filter choice and you cannot clear it from the user interface. To work around this issue for all users, go to the **Database Tool** page (System > Tools > DB Tool) and enter the following SQL query:

  ```
  DELETE FROM master.user_preference WHERE preference_id =
  'event.filter.severity';
  ```

  This issue does not impact the **Event Console** page in the classic user interface.

- 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.
- 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.
- A known issue is causing all report types to fail to generate properly in new OL8 installations.
- Gen 1 SL1 agents that are streaming to Message Collectors will stop displaying uptime after upgrading to SL1 12.1.0. There will be errors in the system log that include "Storage Object Failure due to UNPICKLE ERROR."

  To work around this issue, SL1 administrators can go to the **Database Tool** page (System > Tools > DB Tool) and enter the following SQL query:

  ```
  insert into master.system_custom_config(field, field_value, cug_
  filter) values('collect_sl_streamer', '/opt/em7/bin/python', NULL);
  ```

  After entering the query, click **[Go]**. After the "Enterprise Database: Collector Config Push" process (config_push.py) has time to update your Data Collectors, uptime should once again appear for Gen 1 agent devices.

- "VMware: vSphere Base Pack" PowerPack v306 and v307 are not compatible with Oracle Linux 8 (OL8), which is included in all new installations of SL1 12.1.0. This incompatibility will be addressed in an

upcoming release of the PowerPack in the near future. This issue does not impact SL1 instances that have been upgraded from earlier releases.

- When discovering new Linux devices using "Linux Base Pack" v108, the reclassification of the device fails; devices will remain classified as pingable devices rather than Linux devices. This issue does not impact existing devices that have already been classified.
- In new installations of SL1 12.1.0, 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.
- You cannot delete a PowerPack that has a PowerShell credential. To work around this issue, delete all PowerShell credentials from that PowerPack, and then delete the PowerPack.
- If you repeatedly sign in and out of SL1 in a short period of time, 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:
    - 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.
    - Sign in using the classic SL1 user interface.

  For additional details about this issue, see https://support.sciencelogic.com/s/article/9715.
- If you use CAC with LDAP/AD, then you must define an LDAP service account with permissions that allow the service account to query LDAP before configuring CAC.

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