ScienceLogic

SL1 Hollywood 12.2.4.1 Release Notes

SL1 version 12.2.4.1 (Document revision 1)

SL1 Hollywood 12.2.4.1 Release Notes

IMPORTANT: ScienceLogic strongly recommends that you review the ***upgrade instructions***, important notes about ***upgrading*** SL1, and ***known issues*** for this release before upgrading to SL1 12.2.4.1.

WARNING: SL1 no longer supports the legacy version of Data Pull. If you are upgrading from a version of SL1 prior to 12.2.1.2, you will need to update all of your SL1 appliances to 12.2.4.1, including your Data Collectors and Message Collectors, to avoid potential data loss. When all appliances are successfully upgraded to 12.2.4.1, SL1 will automatically deprecate legacy Data Pull. If you do not update SL1 appliances after 60 days, the data on those appliances will be lost, and you will need to redeploy the appliances.

NOTE: The SL1 Hollywood 12.2.4 release has been removed from the ScienceLogic Support portal and replaced with the 12.2.4.1 release.

These release notes provide a comprehensive list of the features, enhancements, and addressed issues that are included in the SL1 Hollywood 12.2.4.1 release.

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

- *12.2.0*
- *12.2.1.1*
- *12.2.1.2*
- *12.2.3*

This document covers the following topics:

Before You Proceed

If you are planning to consume SL1 Hollywood 12.2.4.1, be advised of the following:

- The 12.2.4.1 release is available only as a patch; there is no ISO version.
- You can upgrade to 12.2.4.1 directly from the following SL1 versions:
    - 12.2.1.1
    - 12.2.1.2
    - 12.2.3

IMPORTANT: If you are currently on SL1 12.1.2, do not upgrade to 12.2.4.1 until ScienceLogic publishes upgrade instructions in a Knowledge Base article.

- The SL1 Hollywood 12.2.4 release has been removed from the ScienceLogic Support portal and replaced with the 12.2.4.1 release.
- STIG-compliant users can upgrade to 12.2.4.1.
- You must currently be on a version of SL1 with all appliances running on Oracle Linux 8 (OL8) before you can upgrade to 12.2.4.1.
- AWS deployments that are using Aurora 3 cannot upgrade to 12.2.4.1.
- Users who currently use Python 3.9 execution environments for Dynamic Applications and Run Book Automations should not upgrade to 12.2.4.1. Due to a known issue, Python 3.9 is not supported in this release. A fix for this issue is planned for a future 12.2.x release.
- After upgrading to 12.2.4.1 and running a security scanning tool against your SL1 appliances, you might experience an issue where the scan lists several "Oracle Linux 8 : container-tools" ELSA security findings. This is due to a known issue that is preventing SL1 from removing certain unneeded packages during the upgrade process for this release. If this occurs, you must *perform a manual workaround to remove those packages*.

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

New Features and Enhancements in SL1 Hollywood 12.2.4.1

Logging

- The ***Session ID*** column was removed from the **Access Logs** page (System > Monitor > Access Logs).

Platform and Security

- SL1 version 12.2.4.1 includes package updates to improve security and system performance. These package updates include the following security update that addresses a known vulnerability: ELSA-2024-7848.

Issues Addressed in SL1 Hollywood 12.2.4.1

Credentials

- Ensured that SL1 data collection using SSH credentials continues authenticating and collecting successfully post-upgrade. (Case: 00466457) (Jira ID: EM-67229)

Data Collection and Retention

- Improved the performance of MySQL queries in systems with a large number of component devices with dynamic component map (DCM) relationships. (Case: 00457073) (Jira ID: EM-66343)
- Addressed issues that were causing unhandled exceptions for inactive interface collection. (Case: 00453285) (Jira ID: EM-66071)
- Resolved an issue that was causing hourly maintenance to end abruptly while updating component device availability statuses. (Case: 00443537) (Jira ID: EM-65600)
- Addressed an issue where the daily maintenance process started in debug mode despite turning it off. (Case: 00353450) (Jira ID: EM-59121)
- Resolved an issue with critical ping-enabled IPv6 devices in Oracle Linux 8 (OL8) versions of SL1 that was causing false outage events to be generated for devices that were known to be online and available. (Case: 00461728) (Jira ID: EM-66608)
- You can now use regular expressions when adding attributes to a realm definition in the /etc/krb5.conf file. (Case: 00445729) (Jira ID: EM-65501)

Device Management

- Addressed an issue that was impacting the ability to configure PHP developer log settings in /opt/em7/backend/silo_php/php_devlog_config.php. (Case: 00434698) (Jira ID: EM-64787)

Discovery

- Interfaces with unexpected characters in its properties do not block SL1 from discovering the device that contains that interface. (Case: 00411856) (Jira ID: EM-62795)
- Resolved an issue that was causing network interfaces to be removed unexpectedly during nightly discovery due to SNMP timeouts or other errors. (Cases: 00387067, 00401470) (Jira ID: EM-61728)

- During SNMP device discovery, SL1 now converts any control characters that are returned for the "sysname" OID to UTF-8 so the characters are properly displayed in the user interface. (Case: 00452024) (Jira ID: EM-66235)

Events

- Events raised for an expired SSL certificate on a device are now properly cleared when the certificate is renewed and an event for this is raised. (Cases: 00316477, 00336592, 00422336) (Jira ID: EM-56192)

Monitoring Policies

- You cannot delete a log monitoring policy in the user interface if that policy is still aligned to a device template. (Case: 00419711) (Jira ID: EM-63550)
- The process of deleting of a log monitoring policy will now complete successfully and automatically update the **Log File Monitoring** page (Registry > Monitors > Logs). (Case: 00416759) (Jira ID: EM-63379)
- Addressed an issue where a duplicate policy was created when a user tried to apply a new Windows service monitoring policy to a device where there is already a policy for the same service. (Case: 00307995) (Jira ID: EM-55205)

System Updates

- Added new timeout handling to the system update staging process. (Case: 00422345) (Jira ID: EM-63897)

Topology

- The Cisco Discovery Protocol (CDP) topology process will no longer stop data collection upon receiving invalid IP addresses. Instead, the CDP process will collect and return data found on the next Cisco device or hardware it finds. (Case: 00422541) (Jira ID: EM-64160)

> **NOTE:** Cisco Discovery Protocol (CDP) allows discovery of Cisco hardware and allows Cisco hardware within the same LAN or WAN to share information about each other.

- Addressed an issue that was causing numerous LLDP topology storage errors due to characters that could not be decoded. (Case: 00431962) (Jira ID: EM-64633)

Recently Deprecated Features

12.2.0

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

- Google Base Pack

> **NOTE:** If you are upgrading from a previous version of SL1, the 12.2.4.1 upgrade will not remove any existing PowerPacks. The PowerPacks listed above are still available for download from the PowerPacks Support page.

12.1.0

- The 12.1.0 release deprecates the following PowerPacks and removes them from the ISO:
    - 3Com Device Classes Base Pack
    - Alcatel-Lucent Base Pack
    - Alteon Monitoring Base Pack
    - APC Base Pack
    - AskEM7 Query Widgets
    - Attachmate Device Classes Base Pack
    - Avaya Base Pack
    - Avocent Base Pack
    - Blue Coat Monitoring Base Pack
    - Brocade: Base Pack
    - Citrix Monitoring Base Pack
    - Citrix: Xen
    - Danaher Device Classes Base Pack
    - DEC Device Classes Base Pack
    - Dell EMC: Isilon
    - Dell EMC: Unity
    - Dell EMC: VMAX and PowerMax Unisphere API
    - Dell OM Base Pack
    - Dell PowerConnect Base Pack
    - Dell PowerVault Event Policies
    - D-Link Device Classes Base Pack
    - EMC: VMAX
    - EMC: VNX

- Empire Device Classes Base Pack
- Enterasys Device Classes Base Pack
- Extreme Base Pack
- Fluke Networks
- Force 10 Monitoring
- Fortinet Base Pack
- Foundry Base Pack
- Google Base Pack
- Hitachi Base Pack
- HP-ISM Base Pack
- HP Pro Curve Base Pack
- HP-UX Base Pack
- Intel Base Pack
- Konica Minolta Base Pack
- LANCOM Systems Device Classes
- Lannair Device Classes
- Lantronix Device Classes
- Liebert Monitoring Base Pack
- Linksys Device Classes
- McAfee Monitoring
- MIB-2 Base Pack
- Microsoft: Azure Classic
- Motorola Device Classes
- NetBotz Base Pack
- NetScout Systems Device Classes
- Netscreen Base Pack
- Nokia Base Pack
- Printer Base Pack
- Riverbed Monitoring
- SMI-S: Array

- SNMP Research Base Pack
- UCD-SNMP Base Pack
- VMware: vSphere Reports
- Vyatta
- Xerox Base Pack

> **NOTE:** If you are upgrading from a previous version of SL1, the 12.2.4.1 upgrade will not remove any existing PowerPacks. The PowerPacks listed above are still available for download from the PowerPacks Support page.

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

11.3.0

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

> **NOTE:** If you are upgrading from a previous version of SL1, the 12.2.4.1 upgrade will not remove any existing PowerPacks. The PowerPacks listed above are still available for download from the PowerPacks Support page.

Upgrading SL1

> **IMPORTANT:** You can consume SL1 12.2.4.1 only if you are upgrading from an earlier SL1 version that ***supports upgrades to this release***. There is no ISO version for version 12.2.4.1.

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

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

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

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

SL1 Extended Architecture

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

Important Upgrade Notes for SL1 Hollywood 12.2.4.1

This section includes important notes for upgrading existing SL1 systems to the Hollywood 12.2.4.1 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 12.2.4.1.

Supported Upgrade Paths

Previous SL1 releases included major updates that you must consume before you can upgrade to 12.2.4.1, if you have not done so already. Therefore, you might be required to upgrade to one or more earlier versions of SL1 before you can upgrade to 12.2.4.1.

You can upgrade directly to 12.2.4.1 from the following SL1 versions:

- 12.2.1.1
- 12.2.1.2
- 12.2.3

If you are currently on SL1 12.1.0.2 or 12.1.1 and all of your appliances are running on Oracle Linux 8 (OL8), you can upgrade to 12.2.1.2 and then to 12.2.4.1.

IMPORTANT: If you are currently on SL1 12.1.2, do not upgrade to 12.2.4.1 until ScienceLogic publishes upgrade instructions in a Knowledge Base article.

Additionally, users on STIG-compliant SL1 deployments can upgrade to this release if they are currently on one of the above versions.

Unsupported Upgrade Paths

You cannot upgrade to SL1 12.2.4.1 in the following scenarios:

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

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

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

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

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

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.

IMPORTANT: If you are upgrading to SL1 12.2.4.1 from an earlier version that used a 10.4.x version of MariaDB, you must also upgrade to MariaDB 10.6.18, as indicated in the table below. ***Before you upgrade MariaDB***, there is an additional procedure you must complete that is documented in the section *Shutting Down MariaDB Before Upgrading*. This step is required ***only*** if you are upgrading from a 10.4.x version of MariaDB to a 10.6.x version.

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?
12.2.4.1 (Upgrade only)	10.6.18	Yes
12.2.3 (Upgrade only)	10.6.18	Yes
12.2.1.2 (Upgrade only)	10.4.31	Yes

SL1 Release	Required MariaDB Version	Requires Appliance Reboot?
12.2.1.1 (ISO only)	10.4.31	N/A
12.2.0	10.4.31	Yes
12.1.2 (OL8)	10.4.31	Yes
12.1.2 (OL7)	10.4.29	Yes
12.1.1 (OL8)	10.4.28	Yes
12.1.1 (OL7)	10.4.29	Yes
12.1.0.2 ISO (OL8)	10.4.28	N/A
12.1.0.2 Upgrade (OL7)	10.4.29	Yes
11.3.2.1	10.4.28	Yes
11.3.2	10.4.28	Yes
11.3.1	10.4.28	Yes
11.3.0	10.4.26	Yes

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

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

Shutting Down MariaDB Before Upgrading

If you are upgrading from a 10.4.x version of MariaDB to a 10.6.x version, then you should perform a slow shutdown of MariaDB ***before upgrading your MariaDB version***.

NOTE: These steps are required ***only*** if you are upgrading to SL1 12.2.3 or 12.2.4.1 and then upgrading from a 10.4.x version of MariaDB to a 10.6.x version. Otherwise, you can skip this section.

To perform a slow shut down of MariaDB:

1. Either go to the console of the Database Server or use SSH to access the Database Server.
2. Run the following command to launch the MySQL prompt:

```
silo_mysql
```

3. From the MySQL prompt, enter the following commands:

```
SET GLOBAL innodb_buffer_pool_dump_pct=100;

SET GLOBAL innodb_buffer_pool_dump_now=ON;

SET GLOBAL innodb_fast_shutdown=0;
```

4. After verifying that each of these settings is correct, you can then proceed with the MariaDB upgrade process that is documented in the section on ***Updating SL1*** in the ***System Administration*** manual.

Aurora 3 Incompatibility

AWS deployments of SL1 on Aurora 3 RDS (MySQL 8.0) are not supported for SL1 12.2.4.1 or earlier. Aurora 3 support is not currently planned for any future SL1 12.2.x releases.

Manual Workaround for 12.2.4.1 Package Issues

A known issue is preventing SL1 from removing certain unneeded packages during the upgrade process for this release. You might encounter this issue after upgrading to 12.2.4.1 and running a security scanning tool against your SL1 appliances if the scan lists "Oracle Linux 8 : container-tools" ELSA security findings.

A fix for this issue is planned for a future release. To work around this issue, you must run a script on the active database appliance to remove the extra packages from the available appliances in your SL1 stack.

To do so:

1. After upgrading your SL1 appliances to 12.2.4.1, download the `remove-docker-ce-rootless.cpython-36.pyc` script from the following ScienceLogic Support knowledge base article: https://support.sciencelogic.com/s/article/15704.
2. Use SSH to access the SL1 Database Server.
3. Type the following command:

```
python3.6 remove-docker-ce-rootless.cpython-36.pyc -v
```

TIP: Depending on the number of appliances in your SL1 stack, this command might take a long time to run. Therefore, ScienceLogic recommends running the script as a background task, and using the `pkg_removal.log` file to monitor the progress from the script. To do so, use the following command instead:

```
nohup python3.6 remove-docker-ce-rootless.cpython-36.pyc -v 2>&1 >
pkg_removal.log &
```

If you want to run the script on a specific SL1 appliance in your stack, you can use the flag `-m <module_id>`, where `<module_id>` is the ID of the appliance. The script also supports the following predefined collections:

- `coll`, `collector`, or `collectors` to specify all SL1 collectors in the stack.
- `cu` or `datacoll` to specify all Data Collectors in the stack.

- `mc` or `messagecoll` to specify all Message Collectors in the stack.
- `db`, `database`, or `databases` to specify all database appliances in the stack.
- `ap` or `adminportal` to specify all Administration Portals in the stack.
- `all` to specify all appliances in the stack.

If you do not use the `-m` flag, the script will automatically run on all patch-eligible appliances in the stack.

For more information about this issue, see https://support.sciencelogic.com/s/article/15704.

Legacy Data Pull Deprecation

As of version 12.2.1.2, SL1 no longer supports the legacy version of data pull. If you are upgrading from a version of SL1 prior to 12.2.1.2, you will need to update all of your SL1 appliances to version 12.2.4.1, including your Data Collectors and Message Collectors, to avoid potential data loss. When all appliances are successfully upgraded to 12.2.4.1, SL1 will automatically deprecate legacy Data Pull. If you do not update SL1 appliances after 60 days, the data on those appliances will be lost, and you will need to redeploy the appliances.

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. The core SL1 platform will switch to Python 3 with the 12.3.0 (Ibiza) release.

However, ScienceLogic will still include Python 2 in parallel with Python 3 until the 12.5.0 (Juneau) release, slated for release in Q2 2025, at which point it will be completely removed from SL1. At that time, customers still using Python 2 in any custom content—including customer-created PowerPacks—will be unable to update to the 12.5.0 (Juneau) release until their custom code is Python 3-compatible.

For more information, see the ***Python 3 Resource Center*** on the ScienceLogic Support site, as well as this knowledge base article: https://support.sciencelogic.com/s/article/12014.

Python 3.9 Execution Environment Issues and Future Support Deprecation

The option to use Python 3.9 execution environments is presently limited to the SL1 12.2.1.1, 12.2.1.2, and 12.2.3 releases.

Users who currently use Python 3.9 execution environments for Dynamic Applications and Run Book Automations should not upgrade to 12.2.4.1. Due to a known issue, Python 3.9 is not supported in this release. A fix for this issue is planned for a future 12.2.x release.

Additionally, the SL1 12.3.0 release will remove support for Python 3.9 entirely and add support for Python 3.11.

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

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

Enterprise Key Management Service (EKMS) Issues

You might experience the following EKMS-related issues upon upgrading to SL1 12.2.4.1:

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

Both of these issues are described in more detail below.

EKMS Configuration File Issues

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

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

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

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

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

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

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

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

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

2. Remove the problematic EKMS files:

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

3. Copy the default `vault_conf` template:

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

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

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

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

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

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

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

6. Re-enable the EKMS services:

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

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

EKMS Remains Encrypted Upon Startup

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

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

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

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

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

1. Decrypt the vault file:

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

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

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

4. Restart the `sl_vault` service:

```
sudo systemctl start sl_vault
```

Global Manager Deployment

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

Obtaining a ScienceLogic Key for Agent RPM Packages

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

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

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

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

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

Validating Agent TLS Connections to the SL1 Streamer Service

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

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

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

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

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

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

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

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

System Update Notes

- ***SL1 updates overwrite changes to the configuration file /opt/em7/nextui/nextui.env***. This is a known issue. (For more details, see https://support.sciencelogic.com/s/article/1161 and https://support.sciencelogic.com/s/article/1423.) ScienceLogic recommends that you back up this file before applying an update and then reapply your changes to this file.
- The SL1 user interface will be unavailable intermittently during system update.
- During the normal system update process, multiple processes are stopped and restarted. This might result in missed polls, gaps in data, and/or unexpected errors. ScienceLogic recommends that you always install SL1 releases during a maintenance window.
- The SL1 system update process starts a background process that can perform any required post-upgrade tasks. The post-patch update process is automatically stopped after 24 hours. However, depending on the size of your database as well as the version from which you are upgrading, the post-upgrade tasks can take several days to perform. If the post-patch update process is stopped after 24 hours, the process will automatically re-start and continue processing from the point at which it was stopped. If you see an event that indicates the post-patch update process was stopped, you do not need to contact ScienceLogic support for assistance until you see the same event for three consecutive days.

Verifying PowerPack Version Compatibility

Before consuming SL1 12.2.4.1, please verify whether any PowerPacks currently running on your system are newer than the PowerPacks included in this release.

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

To avoid spurious error messages:

1. Before installing the SL1 update, go to the **Device Components** page (Registry > Devices > Device Components).
2. Find each root device associated with the PowerPacks you do not want to update and select their checkboxes.

3. Click the ***Select Action*** field and choose *Change Collection State: Disabled (recursive)*, and then click the **[Go]** button.
4. Wait five minutes after disabling collection.
5. Install the SL1 update.
6. After the SL1 update is complete, go to the **Device Components** page (Registry > Devices > Device Components).
7. Select the checkbox for all affected root devices.
8. Click the ***Select Action*** field and choose *Change Collection State: Enabled (recursive)*, and then click the **[Go]** button.

Upgrading from Oracle Linux 7 (OL7) Versions of SL1

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

Known Issues for SL1 Hollywood 12.2.4.1

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

The following known issues exist for SL1 Hollywood 12.2.4.1:

- AWS deployments of SL1 on Aurora 3 RDS (MySQL 8.0) are not supported for SL1 12.2.4.1.
- Users who currently use Python 3.9 execution environments for Dynamic Applications and Run Book Automations should not upgrade to 12.2.4.1. Due to a known issue, Python 3.9 is not supported in this release. A fix for this issue is planned for a future 12.2.x release. (Jira ID: EM-70867)
- When upgrading SL1 on AWS stacks, you might receive an error message that the Data Engines failed to patch correctly. If this occurs, re-run the pre-upgrade tests and then run the patch again; this should result in the Data Engines updating correctly and the correct version then being reflected on the **Appliance Manager** page (System > Settings > Appliances).
- A known issue is preventing SL1 from removing certain unneeded packages during the upgrade process for this release. You might encounter this issue after upgrading to 12.2.4.1 and running a security scanning tool against your SL1 appliances if the scan lists "Oracle Linux 8 : container-tools" ELSA security findings. If this occurs, you must *perform a manual workaround to remove those packages*. (Jira ID: EM-70754)
- After upgrading, to ensure proper data collection, you should go to the **Appliance Manager** page (System > Settings > Appliances), locate one of the Data Collector or Message Collector appliances, and click the lightning bolt icon to force configuration push for that appliance.

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

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

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

  sl1-config -y -q silo CENTRAL ap_user apuser

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

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

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

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

     ```
     sudo visilo
     ```

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

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

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

  (Jira ID: SLUI-18754)

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

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

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

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

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

- After installing or upgrading to SL1 12.2.4.1, each time the system status script (system_status.sh) runs, you might notice that error/traceback messages appear stemming from the SL1 siloupdate service. These messages can be safely ignored. For more information, see: https://support.sciencelogic.com/s/article/11591. (Jira IDs: EM-59277, EM-65832)

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

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

- A known issue might cause several log configuration files to conflict, which could cause you to see errors for the `sl_vault` and `slsctl` logs or potentially block log rotation in some cases, depending on the order in which the files are executed. To work around this issue, delete the config files `~sl_vault` and `~slsctl`. (Jira IDs: SLS-1105, EM-62134)
- When using the SNMP Public V2 credential to discover devices, you might see an unhandled exception in the system log near the end of the discovery session, despite the devices being discovered successfully. (Jira ID: EM-59380)
- The CDP topology process, "Data Collection: CDP Collection," fails because a relevant column, `topology_device_attribute_name`, is missing from the `master.system_settings_core` database table. Because of this issue, no CDP relationships will be created and a Notice-level message relating to CDP topology will appear in the system log. To work around this issue, add the missing column to the Database Server and all Data Collectors:

  ```
  ALTER TABLE master.system_settings_core

  ADD COLUMN topology_device_attribute_name varchar(128) DEFAULT NULL
  COMMENT 'custom attribute name use for topology device name
  matching';
  ```

  (Jira ID: EM-70963)
- A known issue is causing PDF and XSLX Ticketing report types to fail to generate properly due to an OL8 incompatibility issue. For more information, see: https://support.sciencelogic.com/s/article/11649. (Jira IDs: EM-51131)
- After upgrading to 12.2.x, you might be unable to delete devices from the **Devices** page. If this occurs, you can work around this issue by deleting the device from the **Device Manager** page in either the current ("AP2") SL1 user interface (Devices > Device Manager) or the classic user interface (Registry > Devices > Device Manager), or you can delete the device from the Database Server. (Jira ID: EM-62874, Case: 00412497)
- The following known issues impact Business Services:
  - The **[Anomalies]** tab on the **Service Investigator** page for device services might incorrectly display devices that have anomaly detection disabled, rather than showing only those devices with anomaly detection enabled. (Jira ID: EM-62884)
  - Organizations must have at least one or more accounts assigned to them to ensure the relevant services are saved. (Jira ID: SLUI-17810)
  - For services that have their ***RCA Options*** field enabled, and has had a child service removed, SL1 will not compute the health, availability, and risk values until the Service Topology Engine returns an updated topology, which occurs every 5 minutes by default. (Jira ID: SLUI-18853)

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

- In new installations of SL1 12.2.4.1, the "EM7 Web Server" PowerPack that is normally installed by default is not being installed. You can manually install this PowerPack after SL1 has been installed and configured. For instructions, see the section on ***Installing a PowerPack*** in the ***PowerPacks*** manual. This issue does not impact SL1 instances that have been upgraded from earlier releases. (Jira ID: SOL-24609)
- The "Oracle: Database" PowerPack v105 will not work on SL1 12.2.4.1 because of a known issue regarding the Oracle client cx_oracle. This be will addressed in a future release. (Jira ID: EM-64241)
- "VMware: vSphere Base Pack" PowerPack v307 is not compatible with SL1 12.2.4.1 or other SL1 deployments that are running on Oracle Linux 8 (OL8). This incompatibility was addressed in v308 of the PowerPack. (Jira ID: SOL-24062)
- The CyberArk credential gateway service integration is incompatible with SL1's Concurrent PowerShell feature. If you are using the CyberArk credential integration, you must have Concurrent PowerShell disabled. To disable Concurrent PowerShell, go to the **Behavior Settings** page (System > Settings > Behavior), ensure that the ***Enable Concurrent PowerShell Collection*** checkbox is not selected, and click **[Save]**. (Jira ID: EM-63205)
- The **[Expand]** and **[Contract]** buttons are not working as intended on the **Dynamic Application Collections** page (Devices > Device Manager > wrench icon > Collections). You can still expand and contract individual items on the page. (Jira ID: EM-64420)

Copyrights and Trademarks

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

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

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

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

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

Other

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

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

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

International: +1-703-354-1010