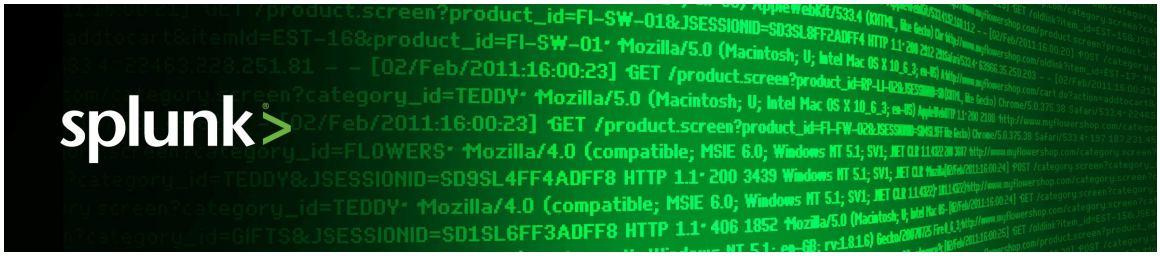

Splunk® Enterprise Installation Manual 7.1.0

About upgrading to 7.1 READ THIS FIRST

Generated: 5/18/2018 11:52 am

About upgrading to 7.1 READ THIS FIRST

Read this topic before you upgrade to learn important information and tips about the upgrade process to version 7.1 from an earlier version.

Splunk App and Add-on Compatibility

Not all Splunk apps and add-ons are compatible with Splunk Enterprise version 7.1. Visit Splunkbase to confirm that your apps are compatible with Splunk Enterprise version 7.1.

If you use Enterprise Security version 5.0.x or earlier, do not upgrade to Splunk Enterprise version 7.1. This version of Splunk Enterprise is not compatible with Splunk Enterprise Security versions 5.0.x and earlier.

Upgrade clustered environments

To upgrade an indexer cluster, see Upgrade an indexer cluster in *Managing Indexers and Clusters of Indexers*. Those instructions supersede the upgrade material in this manual.

To upgrade a search head cluster, see Upgrade a search head cluster in *Distributed Search*. Those instructions supersede the upgrade material in this manual.

Upgrade paths

Splunk Enterprise supports the following upgrade paths to version 7.1 of the software:

- From version 6.5 or later to 7.1 on full Splunk Enterprise.
- From version 6.5 or later to 7.1 on Splunk universal forwarders.

If you run a version of Splunk Enterprise prior to 6.5:

1. Upgrade from your current version to version 6.5.
2. Upgrade to version 7.1.

See About upgrading to 6.5 - READ THIS FIRST for tips on migrating your instance to version 6.5.

Important upgrade information and changes

Here are some things that you should be aware of when installing the new version:

The new Splunk password scheme might affect scripted upgrades

Splunk Enterprise 7.1 introduces a new password scheme for Splunk software users. This scheme includes additional settings and configuration options, which can affect how you upgrade if you use scripts to automate the upgrade process. You might need to change your upgrade scripts before performing scripted upgrades. Specifically, confirm that you do not pass any illegal arguments to the Splunk CLI for starting or restarting Splunk Enterprise during the upgrade, as this could result in a situation where Splunk Enterprise does not start after the upgrade has completed.

The new Splunk password scheme might affect new scripted installations and password usage

While the software retains existing passwords during an upgrade, if you perform scripted installations, those installations might be affected significantly by the new password scheme. You might need to modify your scripts before you perform scripted installations with version 7.1.0 and later of the software. Carefully read the following topics to understand the updated installation process:

- Install on Linux in the *Installation Manual*
- Install on Windows using the command line in the *Installation Manual*

For more information on the updated password policy, see Password best practices for administrators.

Additionally, your Splunk administrator might introduce password eligibility requirements that affect you if you change your password after an upgrade. See Configure Splunk password policies in *Securing Splunk Enterprise* for additional information.

The Splunk Web user interface has been updated significantly

Splunk Web has been refreshed with a new, improved look. While many user interface controls remain the same as they were in previous versions, the interface looks different than before, and some items have been relocated. This might cause confusion for those who have become accustomed to the previous interface.

Data model searches now only use fields that have been defined within the data model

When you upgrade to version 7.1 of Splunk Enterprise, data model searches can only use fields that have been defined within the data model. Splunk Enterprise no longer automatically extracts fields.

Additionally, if you have a data model search that references an automatically extracted field that contains whitespace, you must work around the fact that data models do not allow fields that contain whitespace.

Scheduled views reaper might increase disk I/O and CPU usage on startup

When you upgrade to version 7.1 of Splunk Enterprise, a new process that checks and removes orphaned scheduled views (saved searches or reports that generate PDFs on a schedule) runs. This happens when Splunk Enterprise starts, and might result in increased disk I/O and CPU usage on startup.

The default color scheme for choropleth maps has changed

The color scheme for choropleth maps and single-value visualizations has changed in Splunk Enterprise 7.1. Existing visualizations will be retained through the upgrade, but any new visualizations that you create after an upgrade will use the new color scheme.

HTTP Event Collector now cleans up idle indexer ACK channels by default

After an upgrade to version 7.1 of Splunk Enterprise, the HTTP Event Collector now cleans up any indexer ACK channels it finds that have an idle time of more than 'maxIdleTime' seconds, as defined by that setting in inputs.conf, by default. While this ultimately results in improved HEC performance, you might experience a slight increase in network and CPU activity during the cleanup.

Modified navigation menus in default Splunk apps will be removed after upgrade

After an upgrade to version 7.1 of Splunk Enterprise, any modifications that you have made to navigation menus in default Splunk apps will be removed.

As a reminder, you should not make edits to default apps or configurations, as they can and, in nearly all cases, will be removed after an upgrade. Edit local configurations rather than making modifications to Splunk default configurations and apps.

Stats percentile results might shift by a few percent

(Originally introduced in version 7.0)

Splunk software computes percentiles and median in stats and related commands (`tstats`, `streamstats`, `eventstats`, `chart`, `timechart`, `sistats`, `sichart`, `sitimechart`) using an approximation algorithm (unless you use the `exactperc` aggregation function). Before Splunk Enterprise 7.0, these commands used an approximation algorithm called `rdigest`. After you upgrade, the default digest behavior changes to `tdigest`, which has been shown to be more performant than `rdigest` in some cases, metrics data in particular.

Reports that use percentiles and medians might emit slightly different results upon an upgrade to Splunk Enterprise 7.0. The difference is usually small (less than 1%) but could be greater for highly skewed datasets. After the initial shift, `stats` continues using the new digest method and does not produce another shift unless you switch back to using the `rdigest` method.

If you want, you can revert the digest behavior globally in `limits.conf`. The behavior for `stats`, `tstats`, `streamstats`, `eventstats`, `chart`, and `timechart` are controlled by the setting in the `stats` stanza. The behavior for `sistats`, `sichart`, and `sitimechart` are controlled by the setting in the `sistats` stanza.

See limits.conf.spec in the *Admin Manual*.

The use of disabled lookups in searches or other lookups is no longer allowed

(Originally introduced in version 7.0)

You can no longer use a disabled lookup as part of a search or other lookup. After you upgrade, when you attempt to use a disabled lookup, you receive the error message `The lookup table '<lookup name>' is disabled`.

The ability to customize the number of reports retrieved might reduce browser performance

(Originally introduced in version 7.0)

You can now increase or decrease the number of reports that Splunk Web can retrieve at a time by modifying an entry in `web.conf`. If you increase the number of reports that can be retrieved after you upgrade, you might cause problems with browser performance due to the number of reports available.

A new load-balancing scheme for forwarders is available

(Originally introduced in version 6.6)

All forwarder types now have a new scheme for balancing load between receiving indexers.

In addition to balancing load by time, they can also balance load by amount of data sent. The `autoLBVolume` setting in `outputs.conf` controls this setting.

See Choose a load balancing method in *Forwarding Data* for additional information.

Connectivity over SSL between version 7.0 and version 5.0 and earlier is disabled by default

(Originally introduced in version 6.6)

Because of changes to the security ciphers in version 7.0 of Splunk Enterprise, instances of Splunk software that run on version 5.0 or less cannot connect to instances of version 7.0 or greater by default.

When you upgrade, any instances that run version 5.0 or earlier no longer communicates with the upgraded instance over SSL. For a workaround, you can edit `inputs.conf` and `outputs.conf` on the sending instances to enable ciphers that allow communication between the instances.

For more information, see the Known Issues - Upgrade Issues page in the Splunk Enterprise 6.6.0 *Release Notes*.

Data model acceleration sizes on disk might appear to increase

(Originally introduced in version 6.6)

If you have created and accelerated a custom data model, the size that Splunk software reports it as being on disk has increased.

When you upgrade, data model acceleration summary sizes can appear to increase by a factor of up to two to one. This apparent increase in disk usage is the result of a refactoring of how Splunk software calculates data model acceleration summary disk usage. The calculation that Splunk software performs in version 7.0 is more accurate than in previous versions.

The number of potential data model acceleration searches has increased

(Originally introduced in version 6.6)

The default number of concurrent searches that are used for data model acceleration has been increased from two to three.

If you have an environment that uses data models, that have not yet been accelerated, Splunk software might run up to three searches to accelerate the data models. This can result in increased CPU, memory, and disk usage on the search heads that are accelerating the data models and can also cause more concurrent searches overall in an environment where the search heads are not clustered.

Security changes in SSL and TLS could affect customers who use LDAP

(Originally introduced in version 6.6)

If you have configured Splunk software to use the Lightweight Directory Access Protocol (LDAP) to authenticate, after an upgrade, changes in security settings for Secure Sockets Layer (SSL) and Transport Layer Security (TLS) could prevent the software from connecting to the LDAP server.

If that occurs, you can roll back the updated settings by doing the following:

1. Open `$SPLUNK_HOME/etc/openldap/ldap.conf` for editing with a text editor.
2. Comment the lines that begin with the following:

   ```
   #TLS_PROTOCOL_MIN ...
   #TLS_CIPHER_SUITE ...
   ```
3. Save the `ldap.conf` file and close it.
4. Restart Splunk software.

The 'autoLB' universal forwarder setting in outputs.conf is no longer configurable

(Originally introduced in version 6.6)

The `autoLB` setting, which controls how universal forwarders send data to indexers, and which only had a valid setting of `true`, has been locked to that value. Since auto-loadbalancing is the only way that forwarders can send data, there is no longer a reason to make that setting configurable. Universal forwarders will now ignore attempts to configure the setting to anything other

than `true`.

You might notice an error about a bad configuration for `autoLB` during the startup check. You can safely ignore this error.

The 'compressed' settings on a forwarder and a receiving indexer no longer must match for the instances to communicate

(Originally introduced in version 6.6)

Forwarders and indexers now auto-negotiate their connections. After an upgrade, it is no longer necessary for you to confirm that the `compressed` setting in an `outputs.conf` stanza on the forwarder matches the corresponding `compressed` setting in a `splunktcp://` stanza in `inputs.conf` on the receiver for the forwarder-receiver connection to work.

Indexers in a distributed Splunk environment now respect the INDEXED setting in fields.conf on search heads only

(Originally introduced in version 6.6)

To better align with documented best practice, the way that indexers handle the `INDEXED` setting in `fields.conf` has changed.

Indexers now respect the setting as it has been configured on search heads only. When you upgrade, if you have only configured this setting in `fields.conf` on indexers, you must configure it on the search heads if it is not there.

Use different settings for better data distribution between indexers in a load-balanced forwarder configuration

(Originally introduced in version 6.6)

If you have a setup where universal forwarders have been configured to send data to indexers in a load-balanced scheme, you should replace configurations that have `forceTimeBasedAutoLB` with those that use `EVENT_BREAKER_ENABLE` and `EVENT_BREAKER` instead. For more information about these new settings, see Configure load balancing for Splunk Enterprise in the *Universal Forwarder Manual*.

Protection for the '/server/info' REST endpoint is now on by default

(Originally introduced in version 6.6)

In version 6.5 of Splunk Enterprise, a setting was introduced to require authentication to access the `server/info` REST endpoint.

After you upgrade, this protection is enabled by default.

Memory usage on indexers increases during indexing operations

(Originally introduced in version 6.5)

When you upgrade to version 7.0 of Splunk Enterprise, the amount of memory that indexers use during indexing operations increases. If you have configured an indexer with parallelization (multiple indexing pipelines), the usage increase can be significant.

Indexers that have been configured with a single indexing pipeline, which is the default for a Splunk Enterprise installation, see memory usage increases of up to 10%. Indexers that have two pipeline sets see increases of up to 15%. Indexers that have been configured with four indexing pipelines see increases of up to 25%.

Confirm that your indexers meet or exceed the minimum hardware specifications that the *Capacity Planning Manual* details before you perform an upgrade. See Reference hardware for memory details for each host.

The free version of Splunk now includes App Key Value Store

(Originally introduced in version 6.5)

When you upgrade to version 7.0 of Splunk Enterprise, the free version of Splunk Enterprise gets access to the App Key Value Store feature.

This change results in processes running on your host that support App Key Value Store. These processes might result in extra memory or disk space usage.

The instrumentation feature adds an internal index and can increase disk space usage

(Originally introduced in version 6.5)

The instrumentation feature of Splunk Enterprise, which lets you share Splunk Enterprise performance statistics with Splunk after you opt in, includes a new internal index which can cause disk space usage to rise on hosts that you upgrade. You can opt out of sharing performance data by following the instructions at Share performance data in the *Admin Manual*.

Certain JSChart limits have been increased which might reduce performance in older browsers

(Originally introduced in version 6.5)

The number of series, results, and data points that a JSChart chart element can display has been increased.

The number of series has doubled from 50 to 100. The number of results that can be displayed has increased from 1000 to 10,000. The number of total data points has increased from 20,000 to 50,000.

If you have not already changed the defaults for these JSChart elements, then you will see more data points on your JSChart elements after an upgrade. If you use an older browser to interact with Splunk Enterprise, you might also see slightly reduced performance.

A new capability 'deleteIndexesAllowed' has been added that inhibits index deletion

(Originally introduced in version 6.5)

A new user capability, `deleteIndexesAllowed`, has been added. Non-administrator user roles must hold this capability before they can delete indexes. After you upgrade, you can assign this capability to any non-administrator user roles so that they can delete indexes.

User roles must also hold the "delete_by_keyword" capability to delete indexes.

Windows-specific changes

The Transport Layer Security (TLS) and Secure Sockets Layer (SSL) cipher suites in version 7.1 are not supported on Windows Server 2008 R2

(Originally introduced in version 6.6)

The TLS and SSL cipher suites that come with version 7.0 of Splunk Enterprise do not support Windows Server 2008 R2 by default. If you upgrade, and you used SSL and TLS to handle forwarder-to-indexer communication or alert actions, those actions will not work until you make updates to both Windows and Splunk Enterprise configurations.

See About TLS encryption and cipher suites in *Securing Splunk Enterprise* for instructions on how to configure Windows Server 2008 R2 and Splunk Enterprise to use the new cipher suites.

The Windows Event Log monitoring input has improved performance, new settings, and changes in behavior

(Originally introduced in version 6.6)

The Windows Event Log monitoring input now has improved performance. Owing to improved efficiencies in how the input retrieves and processes events, it provides up to twice the performance as previous versions. To improve performance further, several new input settings have been added. Also, the input now respects the `checkpointInterval` setting in an Event Log monitoring stanza. For additional information about the changes, see Monitor Windows Event Log data in *Getting Data In.*

Before you upgrade:

- Review your Event Log monitoring input stanzas and confirm that the `checkpointInterval` setting is not set to something very large. Large settings might result in a large number of duplicate events after Splunk Enterprise restarts from a crash. If you have not already set `checkpointInterval` then you do not need to set it now.
- Confirm that the machines that retrieve Windows Event Log data meet or exceed the minimum requirements as described in System Requirements for user of Splunk Enterprise on-premises. In particular, if the timely arrival of Event Log events is critical for your organization, any machines that use the input must conform with those requirements.

The Windows universal forwarder installation package no longer includes the Splunk Add-on for Windows

(Originally introduced in version 6.5)

The installation package for the universal forwarder no longer includes the Splunk Add-on for Windows. If you need the add-on, you must download and install it separately.

The installer does not delete existing installations of the add-on.

Support for Internet Explorer versions 9 and 10 has been removed

(Originally introduced in version 6.5)

Microsoft has announced that support for all versions of Internet Explorer below version 11 has ended as of January 12, 2016. Owing to that announcement, Splunk has ended support for Splunk Web for these same versions. This might result in a suboptimal browsing experience in earlier versions of Internet Explorer.

When you upgrade, also upgrade the version of Internet Explorer that you use to 11 or later. An alternative is to use another browser that Splunk supports.

Learn about known upgrade issues

To learn about any additional upgrade issues for Splunk Enterprise, see the Known Issues - Upgrade Issues page in the *Release Notes*.